



MORGAN COUNTY COMMISSION MEETING AGENDA

August 18th, 2026

4:00 WORK SESSION 5:00 REGULAR MEETING

PUBLIC NOTICE is hereby given that the MORGAN COUNTY COMMISSION will hold a regular Commission meeting in the Commission meeting room at 48 West Young Street, Morgan, Utah.

4:00 WORK SESSION

9Line; OBJECTIVE: 9Line respectfully requests the County honor its May 2025 executed leases as written; and will assure expedited issuance of building permits including submitted Tennant Improvements.

5:00 COMMENCEMENT OF MEETING

(A) Opening Ceremonies

1. Welcome
2. Invocation and/or Moment of Reflection: **Hon. Commissioner Fackrell**
3. Pledge of Allegiance

(B) Consent Agenda Items

1. Approval of the Morgan County Commission Minutes from August 4th, 2026.
2. Notice of vacancy on the Morgan County Planning Commission representing Stoddard & Milton – contact Commissioner Wilson if interested in this vacated seat.
3. Weber-Morgan Health Department is launching its 2026 Community Health Assessment.
4. Approval of updates to the Morgan County Information Technology Policies:
 - Policy Library
 - Security Awareness Training Policy
 - Personnel security Policy
 - Access Control Policy
 - PII Protection Policy
 - Media Protection Policy
 - Physical Protection Policy
 - System Information Integrity Policy
 - Incident Response Policy
 - Identification Authentication Policy
 - Configuration Management Policy
 - Risk Assessment Policy
 - Acceptable Use Policy
 - Remote Work Policy
 - Contingency Planning Backup Disaster Recovery Policy

(C) Commissioner Declarations of Conflict of Interest

(D) Public Comments (please limit comments to 3 minutes)

(E) Action Items

1. **Josh Cook** – Discussion/ Decision – County Planning and Zoning
Flagship Homes Development Agreement: A request for approval of County Ordinance **CO 26-17** Flagship Development Agreement for 37 acres in the Mountain Green Area.
2. **Hon. Shaun Rose** – Discussion/ Decision – Morgan County Recorder
Discussion and decision on an agreement with the State of Utah, Division of Technology Services, Utah Geospatial Resource Center (UGRC) to receive Monument Replacement and Restoration Committee (MRRC) funding not to exceed \$24,836. [Budget line 10-4144-320-100]
3. **Janet Christofferson, Esq.** – Discussion/ Decision – Deputy County Attorney
Discussion and decision on her request that Commissioner Nickerson and Commissioner Newton be assigned to work with her to negotiate the next development agreement from inception.
4. **Hon. Garrett Smith** – Discussion/ Decision – Morgan County Attorney
Discussion and decision on a budget adjustment moving monies from the Attorney's payroll and benefits line to the temp legal costs.

MORGAN COUNTY COMMISSION MEETING AGENDA

5. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on entering a grant contract with the State of Utah for “development of public airports FY 2026 pavement preservation project” at the Morgan County Airport not to exceed \$103,765. Morgan Pavement was awarded the pavement maintenance project by the Morgan County Commission on June 16th in the amount of \$91,025. The airport to-date has spent \$4,576.27 in engineering and bid publication. [Budget line 38-4550-260]

6. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on approving the recommended Fall growth grants from the Community and Economic Opportunity (CEO) Board. These pass-through grant funds are part of the Governor’s Office of Economic Development (GOED) Rural Counties Grant. [Budget line 34-4510-340-500]

7. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on change orders for the building addition. Specifically, opening the existing Clerk/Auditor vault into office space for the Records office and building a counter with ADA height and a security door within the Clerk/Auditor’s office. [Budget line 44-4410-310-100]

8. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on a budget adjustment to pay for the new ambulance the Commission ordered in 2025 that should be delivered in November 2026 instead of February 2027. [Budget line 71-2229-000]

9. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on reimbursing Morgala Days Rodeo up to \$1,000 in advertising expenses from the Tourism Tax Advisory Board’s Local Event Fund. [Budget Line 35-4510-409]

10. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on entering into an agreement between the Utah Department of Agriculture and Food (UDAF) for the purpose of Predator Management and committing \$21,100 in costs [50% shall be reimbursed by UDAF, the other 50% are from contribution from local Woolgrowers. This will require a budget adjustment of \$9,700 to account for the pass-through funds. [Budget line 71-2229-000]

11. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on Commissioner registration for the Utah Association of Counties (UAC) Annual Convention September 08-10 at the Utah Valley Convention Center in Provo. Agenda is not yet posted; Registration fee is \$485 per attendee and \$50 for guests. [Budget line 10-4111-230]

12. Kate Becker – Discussion/Decision – Morgan County Administrative Manager

Discussion and decision on Commissioner and presumed Commissioner-Elects registration for the Utah State Association of County Commissioners and Councilmen (USACCC) Conference November 18-20 at the Little America in Salt Lake City. Agenda and registration fees are not yet available. [Budget Line 10-4111-230]

Note: In 2024 Commissioner-Elect Blocker and Nickerson were registered to attend.

(F) Commissioner Comments

- | | |
|-------------------------|-----------------------------------|
| • Commissioner Blocker | • Commission Vice Chair Nickerson |
| • Commissioner Newton | • Commission Chair Wilson |
| • Commissioner Fackrell | |

The undersigned does hereby certify that the above notice and agenda were posted as required by law this **12th** day of **August 2026**.



Kate Becker – Morgan County Administrative Manager

The Commission may vote to discuss certain matters in closed Session (Executive Session) pursuant to Utah Code Annotated §52-4-205. In compliance with the Americans with Disabilities Act, persons needing auxiliary services for these meetings should call Kate Becker at 435-800-8724 at least 24 hours prior to this meeting. This meeting is streamed live.



9Line Work Session
18 August 2026

OBJECTIVE: 9Line respectfully requests the County honor its May 2025 executed leases as written; and will assure expedited issuance of building permits including submitted Tennant Improvements.

ISSUE: building permits with T.I. for Hangar Motel are apparently being held up. Is this characterization correct? If correct, under which County authority is the permit withheld so we can appropriately appeal? For the record, 9Line continues to lose money for delays.

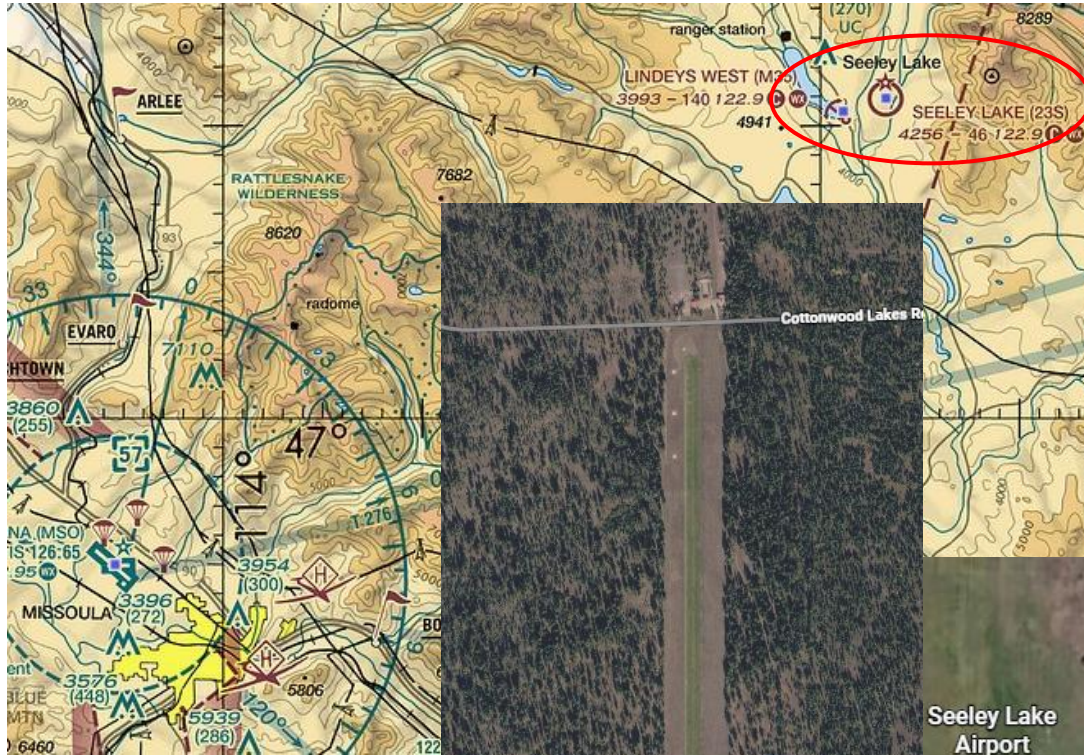
NEW: 9Line had been relying on statements made during the Apr 2025 Commission Meeting regarding its existing CUP. Therefore, 9Line was unaware until 4 Aug 2026, that a new CUP was in fact required. On 6 Aug, 9Line immediately moved to correct by submitting a new CUP application through Civic Review. 9Line is not, nor ever has intended to build a 'Residential Unit'. We have however, intended to construct a 'Lodging Establishment' as defined in Utah Code 29-2-102(5)(f). (Lease: "...short term aviator **lodging** rental...")

AUTHORITIES: Section 6 of the lease was invoked. County legal states 9Line is applying for something illegal and therefore the subject lease-use cannot be honored. How was it determined that the governing ordinance for this project was County Title XV, 155.350? Did 9Line apply to construct a 'Residential Unit'? Can it not be governed under 155.130 since the underlying zone is CB?

Addressing stated concerns:

- Safety: people / kids near airplanes
 - 9Line Aviation Center is at a different elevation from other aprons and therefore has separate access, separate apron, separate parking
 - Morgan Airport historic unfettered access to public
 - Annual Young Eagles event
 - Airport Mgr currently installing signage
- Property Liability: 4 Aug 26 Commission Mtg
 - (USIP?) Doesn't cover airports. County potentially liable for injuries on property.
 - Clarifying Question: how does a Hangar Motel increase injury liability beyond all other normal daily operations at Morgan County Airport? Do transient aircraft notably elevate risk at the airport?
- Precedent - Transient sleeping on airports: lots of examples given at 4 Aug Commission Mtg
 - Following airport slides are both Public and Private (with public access)

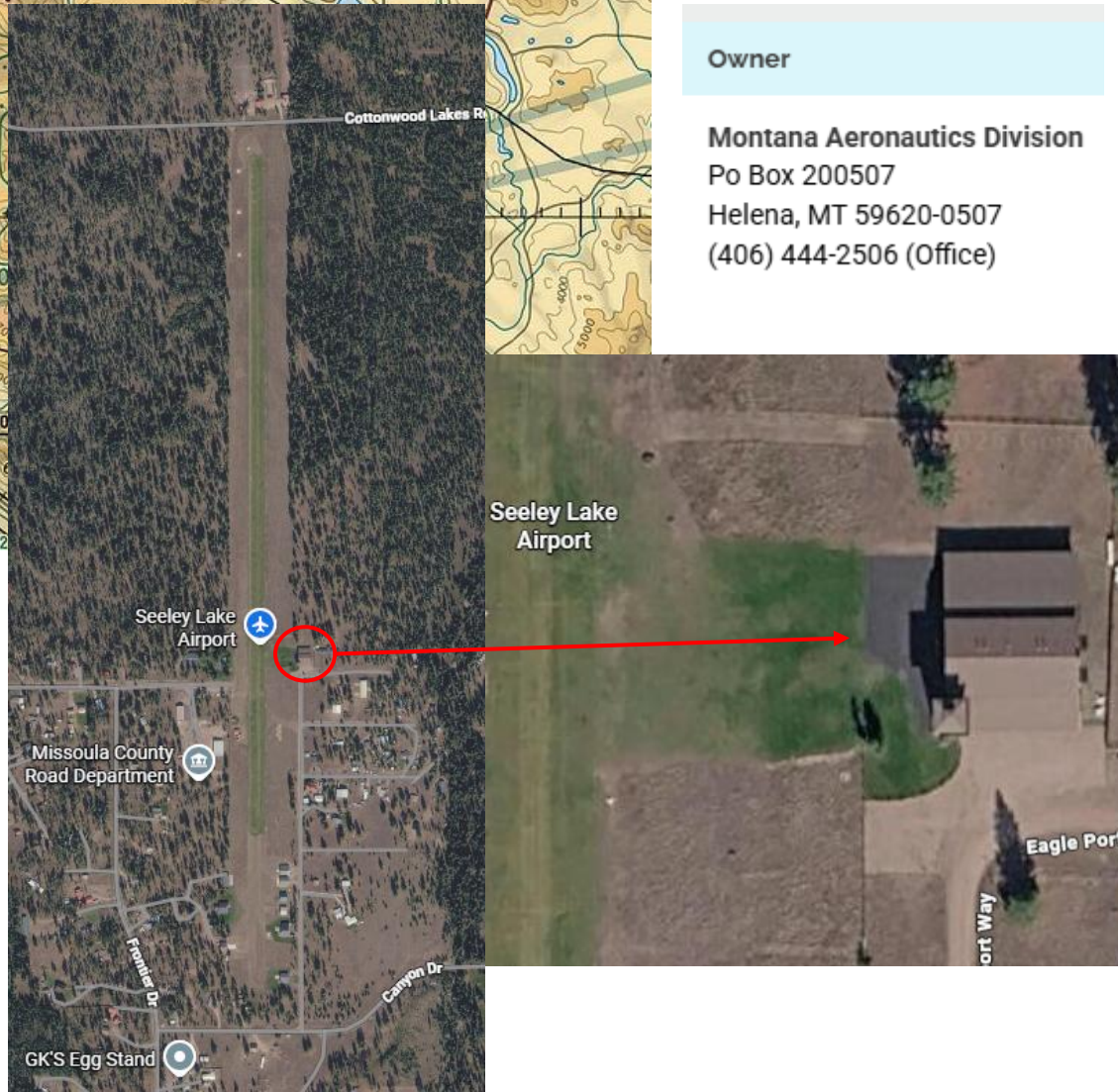
PUBLIC: Seeley Lake, MT



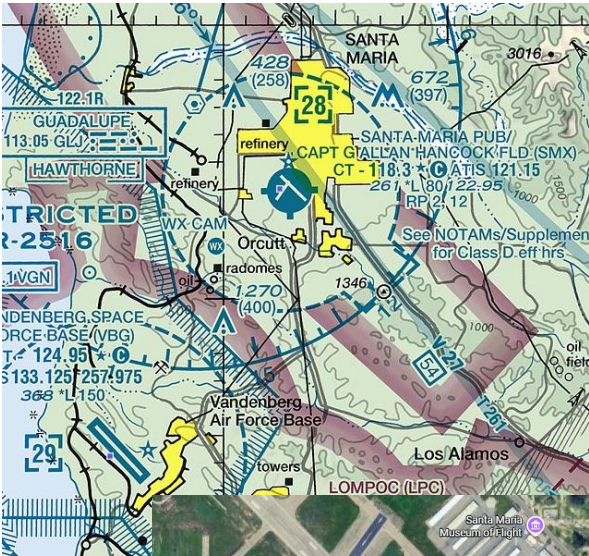
Owner

Montana Aeronautics Division
Po Box 200507
Helena, MT 59620-0507
(406) 444-2506 (Office)

Eagle Port Lodge

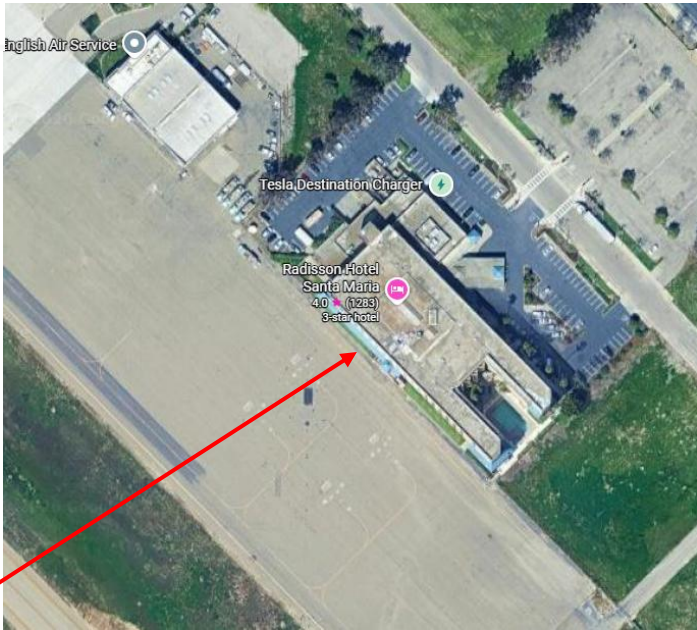
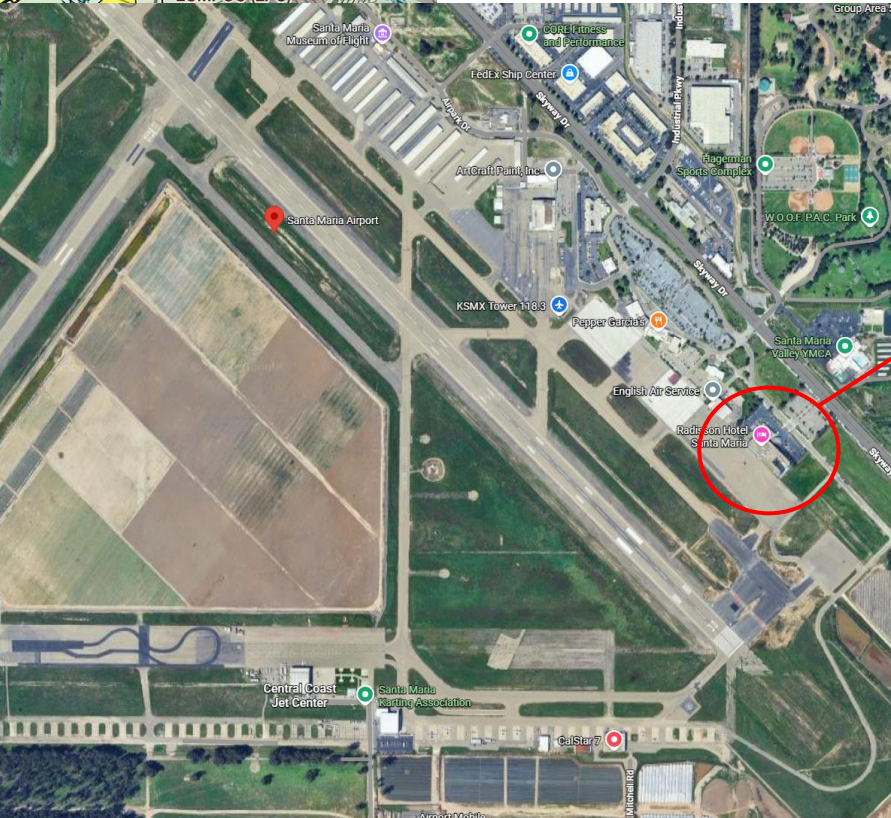


PUBLIC: Santa Maria, CA



Owner

Santa Maria Public Airport District
3217 Terminal Dr
Santa Maria, CA 93455
(805) 922-1726 (Office)

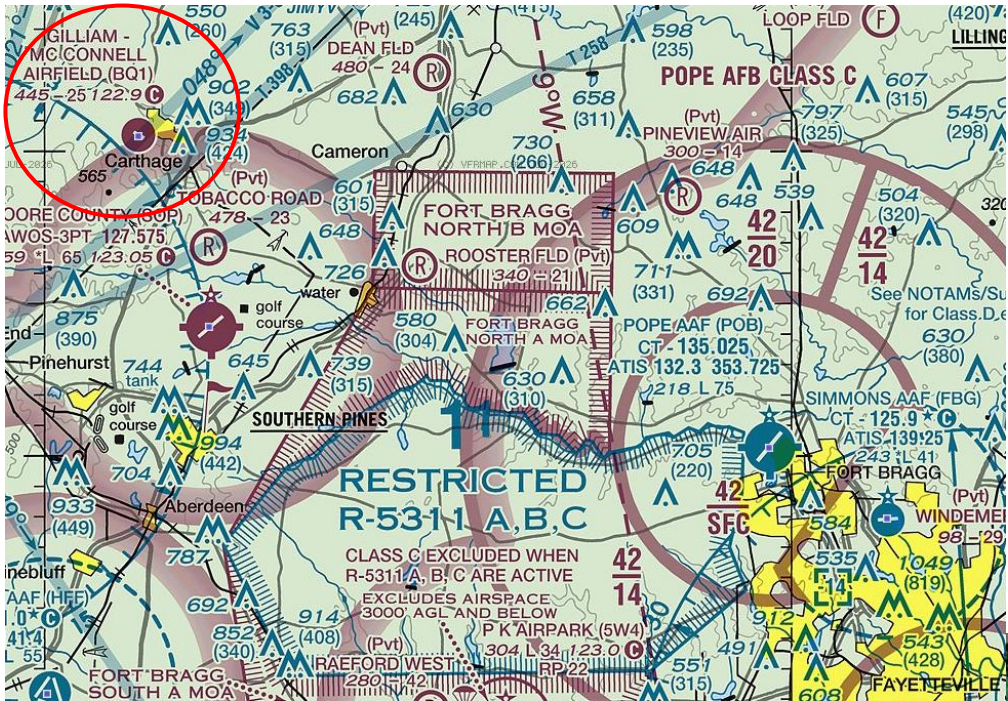


Radisson Hotel



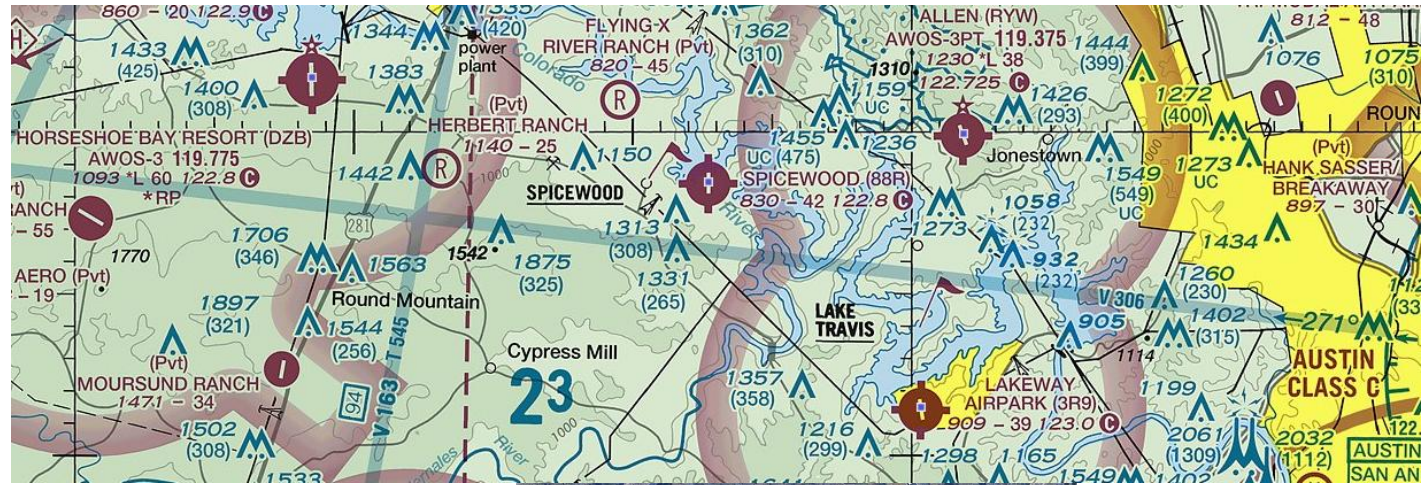
Private Airports that are Open to Flying Public:

- Gilliam-McConnell, NC



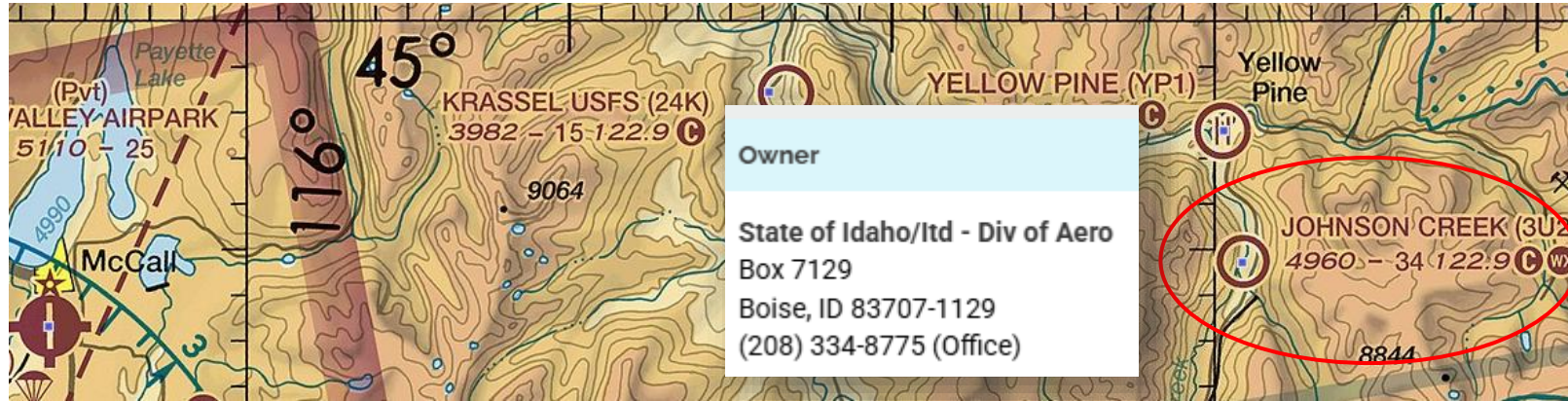
Private Airports that are Open to Flying Public:

- Alpine, WY (46U)
- Horseshoe Bay, TX (DZB)



Private Airports that are Open to Flying Public:

- Johnson Creek, ID





August 4, 2026

4:00 WORK SESSION & 5:00 REGULAR MEETING

PUBLIC NOTICE is hereby given that the MORGAN COUNTY COMMISSION will hold a regular Commission meeting in the Commission meeting room at 48 West Young Street, Morgan, Utah.

COUNTY COMMISSION

Commission Chair Matt Wilson
Commissioner Mike Newton
Commissioner Raelene Blocker
Commissioner Blaine Fackrell
Commission Vice Chair Vaughn Nickerson

OTHER EMPLOYEES

IT Director Jeremy Archibald
Administrative Manager Kate Becker (CAM)
County Attorney Garrett Smith (CA)
County Clerk/Auditor Leslie Hyde
Deputy Clerk/Auditor Chloe Adams
Deputy Clerk/Auditor Penny Butler
Planning and Zoning Director Josh Cook
Planner Kent Page
Deputy Chief Erika White
Chief Brad Wilkes
Code Enforcement Chris Tremea
County Assessor Janell Walker
Mountain Green Fire Marshall Golden Barrett
Attorney Janet Christofferson
County Recorder Shaun Rose

OTHERS IN ATTENDANCE

Debbie Sessions
Tina Kelley
Jeff Mathews
Wanda Adams
Traca Wardell
Jeremiah Cunningham
Sam Nickerson
Amy Everhart
Lillith Allen
Ryan Everhart
Ray Nettleton
Jon Cannon
Brian Nesteroff
Buster Delmonte
Ed Schultz
Brian Brendel
Cynthia Mattson
John Lannefeld
Brandon Green
Jeremiah Cunningham

4:00 WORK SESSION

Flagship BCP Development Agreement Joint Concept Plan and Rezone

Applicant Brandon Green (Flagship Homes) presented a revised concept for the 44-acre Flagship property, proposing 267 units — roughly two-thirds single-family homes and one-third town homes — with smaller lots near the town homes, larger lots to the east, about six acres of open space, a trailhead and trail along Cottonwood Creek, and a clubhouse and amenities to be maintained by the HOA. Under a 2025 Town Center (TC) zone text amendment, the project could reduce its required commercial component to zero if certain conditions are met; the applicant's proposal did so.

Commissioner Newton objected strongly, stating the TC zone was created and intended as a highly commercial zone (originally envisioned at 50% commercial) and that reducing commercial to zero was never the intent, though he credited the applicant for working with neighboring developers to consolidate commercial space. Commissioner Nickerson and Commissioner Blocker both said they never intended the text amendment to eliminate commercial entirely, and Blocker noted that outside economic-development advisors she consulted also recommended against going to zero. Commissioner Fackrell said he now favors keeping the area fully residential but argued the correct path is a formal rezone to a residential or PC zone rather than allowing zero commercial within a TC zone. Chair Wilson pressed the applicant on the project timeline and on whether the amenities offered — a clubhouse, park space, and trail connectivity — adequately offset the loss of commercial space.

County Attorney Garrett Smith clarified that under the TC zone as originally written, the applicant must meet a 35% commercial threshold, but the amended code allows flexibility to trade commercial for other benefits; legally, the application as submitted complies with the amended code, though the Commission retains discretion over whether to accept that trade-off. The applicants urged the Commission to make a decision and

place findings on record rather than continue postponing. The Commission opted to have Commissioners assist the applicant in reaching a revised proposal before its return as a regular agenda item.

5:00 COMMENCEMENT OF MEETING

(A) Opening Ceremonies

1. Welcome
2. Invocation and/or Moment of Reflection: **Hon. Commissioner Nickerson**
3. Pledge of Allegiance

(B) Consent Agenda Items

1. Approval of the Morgan County Commission Minutes from July 21st, 2026.
2. Notice of vacancy on the Morgan County Planning Commission representing Stoddard & Milton – contact Commissioner Wilson if interested in this vacated seat.

Commissioner Newton moved to approve all consent agenda items.

Seconded by Commissioner Nickerson

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

(C) Commissioner Declarations of Conflict of Interest

Commissioner Wilson declared a conflict of interest on Item 5 (Buster's VRBO).

(D) Public Comments (please limit comments to 3 minutes)

Golden Barrett (Fire Marshal, Mountain Green Fire Protection District): spoke in support of the Flagship development, noting the applicant's agreement to provide property for a future fire-station expansion to support full-time staffing. He also addressed Item 5 (Buster's VRBO), stating that fire and building code generally do not independently restrict a use in a given area — that determination comes down to zoning.

Chair Wilson acknowledged feedback that he keeps a relatively informal atmosphere at the podium and stated he would aim to keep the meeting more orderly going forward, while still allowing latitude for open commission discussion.

(E) Action Items

1. Emergency Management Director Erica White – Discussion/Decision – Interlocal Response

Discussion and decision on an entering into an interlocal cooperation agreement with North Summit Fire District regarding paramedic transport services.

Emergency Management Director Erica White explained the agreement formalizes an existing working relationship: North Summit now staffs paramedic-level service and will be billed quarterly only when its paramedics transport a patient in Morgan County, so cost is not passed on to residents unless the service is used. Commissioner Nickerson noted the agreement addresses resident questions about why North Summit responds in Morgan County and confirmed it improves response coverage on the county's north end. Commissioner Fackrell asked whether the agreement was reciprocal; Ms. White clarified that Morgan County does not charge for fire (as opposed to EMS/paramedic transport) response under the existing statewide mutual aid compact, so North Summit does not separately owe Morgan County under this specific agreement, though the county already recoups its own costs whenever it transports patients into North Summit's district.

Commissioner Newton moved to approve the interlocal cooperation agreement with North Summit Fire District regarding paramedic transport services.

Seconded by Commissioner Fackrell

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

2. Josh Cook – Discussion /Decision – County Planning & Zoning

Wasatch Peaks Ranch (WPR) Phase 6B Final Plat: A request for approval of final plat for Wasatch Peaks Ranch Phase 6B in the Peterson area.

This is a 16-lot single-family subdivision; the Planning Commission approved the preliminary plat for Phase 6B (together with Phase 6D) on March 26, 2026. Ed Schultz, a representative for Wasatch Peaks Ranch, presented the final plat. Commissioner Fackrell asked about shared driveway access to several interior lots and about a trail/ski-run corridor shown crossing multiple lots; Brian, another Wasatch Peaks Ranch representative, confirmed shared driveway access is provided via the previously approved Phase 6A plat, and that the area alongside the ski run is part of each adjoining lot but is recorded and restricted as open space.

Commissioner Nickerson moved to approve the WPR Phase 6B Final Plat.

Seconded by Commissioner Blocker

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

3. Josh Cook – Discussion /Decision – County Planning & Zoning

Wasatch Peaks Ranch (WPR) Phase 6D Final Plat: A request for approval of final plat for Wasatch Peaks Ranch Phase 6D in the Peterson area.

Staff presented this 5-lot single-family subdivision, also recommended for approval by the Planning Commission on March 26, 2026. Commissioner Fackrell asked about a wetland area shown on one of the lots; Ed Schultz (Wasatch Peaks Ranch) and Administrative Manager Kate Becker confirmed the wetland/open-space portion is not buildable and confirmed the acreage in that phase is not eligible to be placed back into greenbelt status, as all of Phase 6 has previously been removed from greenbelt.

Commissioner Newton moved to approve the WPR Phase 6D Final Plat.

Seconded by Commissioner Blocker

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

4. Hon. Commissioner Matthew Wilson – Discussion/ Decision – Commissioner Request

“Many complaints of our policy to assume home bought and built are secondary residence and taxed that way unless proven otherwise, should be just the opposite. This will over burden the BOE and is unnecessary. [No supporting documents submitted with request.”; Statute attached for reference]

Commissioner Wilson raised concerns from residents who have lived in their homes for many years and recently received notices requiring them to file a primary-residence declaration or be taxed as a secondary residence, expressing concern that elderly and other residents may not understand the notice or the appeal process, and that the volume of resulting Board of Equalization (BOE) appeals is burdensome.

County Assessor Janell Walker and Administrative Manager Kate Becker explained that state law (not a policy originated by the current Assessor) requires the county to obtain a signed primary residential exemption (PRE) declaration on file for each parcel receiving the exemption, and that a 2003 county ordinance implementing this has been enforced inconsistently in the past. Without a signed declaration on file, the state could audit the county and "claw back" up to three years of exempted tax value. Residents who miss the standard filing deadline retain the right to file a late appeal through the BOE process; the Assessor's office reported having already corrected 18 cases in the current cycle and stated it has not reclassified any long-term resident's home to secondary status without cause. Commissioner Newton noted the exemption does not change the county's total tax revenue but shifts the tax burden among property owners, making accuracy important. The Assessor noted a new state law takes effect January 1, 2027, making the declaration requirement uniform statewide and removing individual county discretion. Commissioner Fackrell asked whether Ms. Walker could provide commissioners a list of residents who have not yet filed so they could assist constituents directly; County Attorney Garrett Smith cautioned commissioners selectively contacting individual residents, recommending instead a public information effort (e.g., county website or social media).

No motion was made and no vote was taken on this item; it was discussion only.

5. Hon. Commissioner Matthew Wilson – Discussion/ Decision – Commissioner Request

"Discussion and decision on CUP for Busters VRBO hangar. Being held up by attorney with no letter or phone call to explain the reason." [No supporting documents submitted with request]

Commissioner Wilson raised a commissioner request regarding a CUP for a hangar remodel at the Morgan airport. Buster Del Monte at the Morgan County Airport raised concerns to Commissioner Wilson describing delays and lack of communication from the County Attorney's office; Wilson also addressed and rejected public social-media criticism directed at him personally on the matter and disclosed his own prior conflict of interest and abstention on a related earlier vote.

County Attorney Garrett Smith responded that the criticism of him personally was unwarranted, and reminded the Commission that mutual respect should go both ways — noting that Assessor Janell Walker had similarly felt attacked earlier in the meeting, and that the Commission should hold itself to the same standard of civility it expects of the public. Garrett Smith then clarified his role and responsibilities as County Attorney: on the civil side, he enforces the Open Meetings Act, manages executive sessions, vets ordinances and resolutions, reviews and approves contracts and agreements, advises the Commission on legal risk, and defends the county against claims; he also carries criminal prosecution duties. He stated that advising individual residents or business owners on how to make their private business work is not part of his role, and that when he provides legal guidance, his priority is defending the county's interests rather than any individual applicant's. He further noted no CUP application specific to this VRBO use has actually been filed, and that his office cannot be said to be "holding up" an application that does not yet exist.

Commissioners Newton, Nickerson, Blocker, and Fackrell each gave their views. Newton said if code prohibits the use, the existing lease language allowing it should be revised; if no code prohibits it, the county should honor what was agreed. Commissioner Nickerson had his son, Sam Nickerson, report his research into other airports' practices (including a hotel operated on a public airport in Colorado) and expressed general support for allowing limited, low-impact use, tied to the county's practice of keeping airport-generated revenue within the airport fund; he also questioned why a short-term rental requires a business license but is not treated as a commercial use under county code. Blocker expressed concern that permitting an Airbnb-style use sets a precedent, raises liability questions, and was not what she understood the commission to have approved when it granted the original CUP (which she understood to cover overnight storage of aircraft, not lodging for people). Fackrell supported allowing the use, citing past efforts to increase airport revenue and reduce the general fund's subsidy of the airport, and stated that in his own view, any activity conducted for profit — including a home-based business — is inherently a commercial use regardless of the zone it occurs in.

Deputy Clerk/Auditor Chloe Adams stated that if a business license application for this type of short-term rental came to her desk, she would deny it based on the county's current code, consistent with her training through the Utah Business License Association. Planning Director Josh Cook explained that short-term rentals are treated as a residential use under county code (distinct from a home occupation permit/business license for a business operated inside a residence), and that hotels and motels — unlike short-term/VRBO rentals — are separately permitted uses within a commercial buffer zone.

County Attorney Garrett Smith advised that a CUP is a separate process from a lease, and that a lease does not itself grant a CUP; no CUP authorizing short-term residential rental currently exists for this hangar. He further explained that the airport is zoned as a commercial buffer zone, which does not permit residential uses of any kind, and that under Morgan County's short-term rental code, a short-term vacation rental is defined as a residential unit (or portion of one) rented for fewer than 30 consecutive days — a definition that only applies to residential units in residential zones. Because there are no residential units on the airport, he advised that short-term/VRBO-style rentals are not permitted there under current code, regardless of lease terms, and that a code text amendment would be required to allow the use. He distinguished this from hotels and motels, which are permitted in the commercial buffer zone but are not "apples to apples" with a VRBO, since hotels have full-time staff and are not classified as residential use. The applicant (Buster Del Monte) stated he believed the use was covered under his existing CUP based on prior public statements, including from the County Attorney. Planning Director Josh Cook separately noted the applicant is currently out of compliance with certain existing CUP conditions (including a required water-will-serve letter), which is a separate matter from tonight's discussion.

No motion was made and no vote was taken on this item. The Commission agreed to hold a future work session to discuss options with the applicant.

6. Hon. Commissioner Matthew Wilson – Discussion/ Decision – Commissioner Request

Discussion and decision on a motion to reconsider pursuant to Morgan County Resolution CR 26-03 'Commission Rules of Order and Procedure,' Rule VIII (10); Motion for reconsideration is a vote on action item 6 from the June 16th Commission Meeting regarding the "P-C Zoning Code Text Amendment."

Procedural Note: *If motion to reconsider is approved, the action item will be brought back for discussion and decision at the next scheduled County Commission meeting.*

Administrative Manager Kate Becker explained that only a commissioner who voted on the prevailing (denying) side of the original motion may bring a motion to reconsider. Commissioners Wilson, Newton, and Nickerson had voted on the prevailing side; Wilson stated he cannot make motions as chair, Newton stated he did not wish to make the motion, and Nickerson stated he was not prepared to make a motion at this meeting but wanted time to consider potential safeguards before revisiting the ordinance. **Commissioner Newton** reiterated concern that any change to the code would apply to all qualifying parcels countywide, not just the one project under discussion.

No motion to reconsider. No vote was taken.

7. Hon. Shaun Rose – Discussion/ **Public Hearing /Decision – Morgan County Recorder**

Discussion and decision on County **Ordinance CO 26-16** Morgan County Monument Preservation Ordinance. This ordinance creates a consistent process for Monument Encroachment Permits and Monument Construction Permits, requires Monument Tie Sheets to improve future monument recovery, and updates the administration of the existing Public Land Corner Preservation Fund.

Procedural Note: *The two Resolutions in the packet with this Ordinance are for illustration only and will be passed at a future Commission meeting.*

County Recorder Shaun Rose, with contracted county surveyor Jeremiah Cunningham, presented the ordinance, explaining it establishes a permitting process for monument encroachment and construction, requires monument tie sheets, updates the Public Land Corner Preservation Fund, and places the cost and responsibility for monument protection and replacement on developers rather than general taxpayers. Mr. Rose gave a specific example of an existing subdivision (in the Mountain Green/Cottonwood area) currently held up because a section-corner monument was destroyed during construction; the ordinance would require the party responsible to install and document reference monuments before further approvals proceed. Mr.

Cunningham reported roughly 800 monuments countywide, with replacement costs historically ranging from about \$1,800 to \$4,500 each, funded in part through a state monument-restoration grant program. Commissioner Nickerson noted the ordinance would place monuments deeper underground in agricultural areas to withstand plowing. Ordinance fees themselves were not adopted with this ordinance, as fee adoption requires a separate public hearing; two related resolutions in the packet were presented for illustration only and will be considered at a future meeting. Following the hearing, Recorder Rose also requested that staff be directed to review related ordinances for consistency; Planning Director Josh Cook noted he cannot initiate that review without Commission direction, and the Commission verbally directed staff to proceed.

Commissioner Nickerson moved to go to public hearing
Seconded by Commissioner Blocker

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

Commissioner Newton moved to close the public hearing and reconvene the regular meeting.
Seconded by Commissioner Fackrell

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

Commissioner Nickerson moved to approve Ordinance CO 26-16, the Morgan County Monument Preservation Ordinance.

Seconded by Commissioner Fackrell

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

8. Josh Cook – Discussion/ [Public Hearing](#) /Decision – County Planning and Zoning

Flagship Homes Development Agreement: A request for approval of County Ordinance **CO 26-17** Flagship Development Agreement for 37 acres in the Mountain Green Area.

Brandon Green summarized the proposal for the public record: a single-family and town-home development of up to 267 units, with town homes concentrated on the west end transitioning to larger single-family lots on the east; a trailhead parking area, creek crossing, and paved trail along Cottonwood Creek; one of two proposed pickleball courts open to the public; a clubhouse (approximately 2,000 square feet) reserved for residents; and property proposed to be deeded to the Mountain Green Fire Protection District for a station expansion. The proposal would reduce the required commercial component to zero under the town-center (TC) zone text amendment. A related rezone request for adjoining acreage is a separate matter proceeding through the Planning Commission and was not part of this hearing.

Commissioners raised concerns about development-agreement language allowing the applicant to adjust the unit mix (between town homes and single-family homes) up to the 267-unit cap without formally amending the agreement; Commissioner Newton and Commissioner Blocker asked for a firmer cap on how much the

mix could shift without returning to the Commission. Planning Director Josh Cook noted the county's standard PC-zone amendment provision (allowing minor changes up to 5%) could be incorporated; the applicant agreed to work with staff to add that limit. Commissioner Blocker stated she was not prepared to support the agreement without a defined framework for how much commercial value the county would be giving up in exchange for the proposed amenities.

Commissioner Nickerson moved to enter public hearing.

Seconded by Commissioner Newton

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

Public Comment:

Lilia Allen (Mountain Green): stated she did not believe the proposed amenities were a fair trade-off for the community.

John Lannefeld (Cottonwoods area, 40-year Mountain Green resident): opposed further town-home development, stating the community cannot sustain additional units of that type and citing worsening traffic on Old Highway.

Zach Burton (Mountain Green): argued that single-family homes are not an equivalent tax-base substitute for commercial development and questioned the proposed trade-off of amenities in exchange for eliminating the commercial requirement.

Tyler Nelson (Mountain Green, Mountain Green Fire Department): spoke in support of the project, citing its benefit to the fire department.

Jennifer Lance (Mountain Green): urged the Commission not to approve the project without a commercial component.

Ryan Everhart (Mountain Green): stated that if the property is going to be developed as residential, it should be zoned residential rather than granted an exception within the town-center zone.

Commissioner Blocker moved to leave public hearing

Seconded by Commissioner Fackrell

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

Planning Director Josh Cook clarified after the hearing that, because this item concerns an existing development agreement rather than a rezone, it should technically have been noticed as a public meeting rather than a public hearing; the actual rezone-related public hearing will occur separately before the Planning Commission. The Commission continued discussing whether the applicant should be held to the 35% commercial standard versus an all-town-home layout, agreeing the outcome need not be all-or-nothing and that the applicant could return with a revised, negotiated proposal. The applicant and Commission agreed to hold an additional work session, with the applicant submitting a list of proposed "substantial" commercial/amenity concessions in advance; a follow-up work session was scheduled for Monday, August 10 at 4:00 p.m.

Commissioner Newton moved to postpone Item 8, the Flagship Homes Development Agreement, to the August 18, 2026 meeting.

Seconded by Commissioner Nickerson

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

9. Josh Cook – Discussion/ **Public Hearing** /Decision – County Planning and Zoning

3rd Amendment to the Cottonwoods DA, PRUD, and Overlay Report: A request for approval of Morgan County Ordinance **CO 26-02** pertaining to the third amendment of the Cottonwoods Development Agreement, Cottonwoods Planned Residential Unit Development (PRUD) Ordinance, and the Cottonwoods Overlay Report.

This was noticed for Public Hearing for the February 17th, 2026 Commission meeting and at that meeting was continued to a-date-certain being May 19th, 2026. At the May 19th, 2026 it was continued to a-date-certain being July 7th. At the July 7th, 2026 it was continued to a-date-certain being August 4th, 2026.

Commissioner Nickerson moved to postpone Item 9 to the first meeting in September (September 1, 2026), with Commissioners Blocker and Wilson assigned to work with the applicant.

Seconded by Commissioner Fackrell

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

10. Hon. Garrett Smith– Discussion/Decision – Morgan County Attorney

Discussion and decision on an amendment to the Exclusive Right-of-Way Easement Grant between Morgan County and Questar Gas Company previously approved at the July 7th, 2026, Commission meeting. Questar is now requesting that section five been removed from the final easement grant.

Attorney Garrett Smith recommended against removing Section 5, explaining that because the easement is exclusive — restricting the county's own access to and control over the property — removing the indemnification language would leave the county holding liability for a property it cannot access, maintain, or monitor, without a corresponding benefit.

Commissioner Newton moved to reject the amendment to the agreement with Questar Gas company requesting exclusive right-of-way easement.

Seconded by Commissioner Blocker

VOTE:

Commission Chair Wilson: Aye

Commissioner Newton: Aye

Commissioner Blocker: Aye

Commission Vice Chair Nickerson: Aye

Commissioner Fackrell: Aye

The vote was unanimous. The motion passed.

(F) Commissioner Comments:

Commissioner Blocker: Reported on the UAC annual convention (September 9–10) and asked **Kate Becker** to register attendees; discussed a possible Browning firearm for a convention basket/drawing; said the fair and rodeo were well received, with positive feedback on assigned seating; reported meeting with Celeste Malloy at the fairgrounds regarding I-84, and with the Northern Utah Economic Alliance Board, which will help the county build a real estate database for market analysis.

Commissioner Fackrell: No comments recorded, other than fair-related parking discussion addressed under Commissioner Newton's comments below.

Commissioner Nickerson: Called the fair the highlight of the week despite the heat, and invited public feedback ahead of a debrief. Raised concern that members of the public are operating businesses (e.g., paid training courses, private lessons) out of county amenities such as the rifle range and pickleball courts without the intended community access or any compensation to the county. Also raised similar concern regarding private airport hangar tenants subleasing hangar space for profit at low county-set rates, noting that airport-generated revenue stays within the airport fund; asked whether the county should consider a fee structure to recoup value from these uses. Noted the Airport Advisory Board is scheduled to discuss the issue and may draft a letter to the Commission.

Commissioner Wilson: Thanked staff and volunteers for their work on the fair; clarified he did not intend to question County Attorney Garrett Smith's integrity earlier in the meeting and was frustrated with timing, not with him personally; said the primary-residence declaration issue (Item 4) came to his attention through resident complaints, including from his own mother, and that the notice/process is not easy for elderly or first-time homeowners to navigate.

Commissioner Newton: Thanked fair volunteers, county staff, and public works for a successful event, noting strong Friday and Saturday attendance; reported the new sound and screen system performed well and that improved power infrastructure eliminated the need for generators, aside from an unrelated city power outage; noted the county should acquire additional spider boxes and extension cords for future events. Raised ongoing concerns about unauthorized camping and resource use at the fairgrounds, and about individuals conducting paid riding lessons or similar business activity in county arenas without paying for facility use, calling it an unfair subsidy by residents. Discussed with **Commissioner Fackrell** possible adjustments to fair parking layout (tightening rows, using the barefoot-tubing lot) to increase capacity next year.

Commissioner Fackrell moved to adjourn at 9:24 p.m.

Seconded by Commissioner Newton

APPROVED: _____ DATE: _____
Morgan County Commission Chair

ATTEST: _____ DATE: _____
Morgan County Deputy Clerk/ Auditor

In compliance with the Americans with Disabilities Act, persons needing auxiliary services for these meetings should call Kate Becker at 435-800-8724 at least 24 hours prior to this meeting. This meeting is streamed live.

If you want to participate virtually in any public comment listed on this agenda, you need to contact Jeremy@morgancountyutah.gov at least 48 hours before the scheduled meeting.



48 W Young St - 886
Morgan, UT 84050

Morgan County
Planning & Development
Services

NOTICE

Morgan County Commissioner Matthew Wilson is seeking applicants to fill the vacated Stoddard & Milton seat on the Morgan County Planning Commission.

If no suitable applications are received the positions may be filled by the County Commission at their discretion.

Interested individuals may obtain an application at www.morgancountyutah.gov or may reach out directly to Commissioner Wilson at mwilson@morgancountyutah.gov (801) 725-4457

Seat to be recommended for appointment on July 21st, 2026. All interested persons should contact Commissioner Wilson no later than Monday July 13th by 5pm MST.

**TAKE THE
2026 WEBER-MORGAN
HEALTH DEPARTMENT
COMMUNITY HEALTH
ASSESSMENT!**



The Weber-Morgan Health Department is excited to launch the 2026 Community Health Assessment (CHA), and we are asking for your help to reach the communities you serve.

The Community Health Assessment is conducted every three years to understand the current health, strengths, needs, and experiences of residents throughout Weber and Morgan Counties. The information gathered will help identify community priorities, guide future health improvement plans, and inform how resources and services are directed across our communities. Take the survey

here: <https://survey.alchemer.com/s3/8856766/WMHD-CHA>

We invite you to:

- Have your household represented by taking the survey.
- Share the survey with your staff, clients, members, and network in Weber and Morgan Counties.
- Display flyers in your lobby, office, or community spaces. (attached in English and Spanish)
- Share the survey through newsletters, social media, or other communication channels.

Who should participate?

We are asking **one adult (aged 18 years or older) from each household** to complete the survey. To help insure a representative sample, we ask that the adult **whose birthday is closest to the day the survey is completed** be the one to respond.

Participant Incentives

As a thank you for participating:

- The first 400 eligible households will receive an electronic \$10 gift card.
- All eligible households will be entered into a drawing for one of ten \$100 electronic gift cards.

Your partnership is essential to ensure we hear from residents across Weber and Morgan Counties! The more voices and experiences that are shared, the better equipped we will be to help identify community strengths, address emerging challenges and gaps, and improve the health of our communities.

Morgan County Information Technology Policies & Procedures MCIT-001 through MCIT-015

Document Series: MCIT-001 – MCIT-015

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

	Page
• MCIT-001 – Security Awareness & Training	2
• MCIT-002 – Personnel Security	11
• MCIT-003 – Access Control	24
• MCIT-004 – PII Protection	35
• MCIT-005 – Media Protection	45
• MCIT-006 – Physical Protection	54
• MCIT-007 – System and Information Integrity	63
• MCIT-008 – Incident Response	74
• MCIT-009 – Identification & Authentication	82
• MCIT-010 – Configuration Management	93
• MCIT-011 – Audit & Accountability	104
• MCIT-012 – Risk Assessment	115
• MCIT-013 – Acceptable Use	125
• MCIT-014 – Remote Work	135
• MCIT-015 – Contingency Planning, Backup & Disaster Recovery	144

Purpose of this Policy Library

This document library establishes Morgan County's Information Technology policies and procedures supporting cybersecurity, privacy, operational security, the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, NIST SP 800-53 Rev. 5, and other applicable legal and regulatory requirements. Each policy is intended to function as a standalone document while collectively providing a comprehensive information security governance framework.

Morgan County Security Awareness & Training Policy & Procedures

Document Number: MCIT-001

Version: 3.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Security Awareness & Training Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements for security awareness education and role-based training to ensure County personnel understand their responsibilities for protecting County information and Criminal Justice Information (CJI).

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Awareness and Training (AT) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County employees, elected officials, contractors, volunteers, interns, and any individual granted access to County information systems or facilities.

4. Objectives

Provide initial and recurring security awareness training, promote secure behavior, satisfy CJIS requirements, and reduce cybersecurity risk through education.

5. Definitions

Key terms include Security Awareness, Role-Based Training, CJI, Phishing, Social Engineering, and Acceptable Use.

6. Security Awareness & Training Policy

The following requirements establish the minimum-security awareness and training requirements for Morgan County personnel.

6.1 Initial Training

Personnel shall complete security awareness training before or as soon as practicable after being granted access to County information systems.

6.2 Annual Refresher Training

All personnel shall complete security awareness training at least annually.

6.3 Role-Based Training

Personnel with specialized security responsibilities or CJI roles shall receive training appropriate to their duties before performing those duties or receiving the related CJI access and at least annually thereafter.

6.4 CJIS Security Awareness

Personnel requiring access to CJI shall complete CJIS-required security awareness training before accessing CJI and at least annually thereafter. The Terminal Agency Coordinator (TAC) identifies and coordinates CJIS-specific training and testing requirements, while Information Technology administers assignments and maintains completion records.

6.5 Acceptable Use

Training shall address acceptable use of County information systems and technology resources.

6.6 Phishing & Social Engineering

Training shall include recognition and reporting of phishing, social engineering, and related threats.

6.7 Incident Reporting

Personnel shall be trained to report suspected security incidents immediately and no later than one (1) hour after discovery through approved County reporting channels.

6.8 Privacy & PII

Training shall address protection of Personally Identifiable Information and other sensitive information.

6.9 Policy Acknowledgement

Personnel shall acknowledge applicable security policies when required.

6.10 Training Records

Information Technology shall document and monitor training completion. Individual CJIS training records shall be retained for at least three (3) years, and other training records shall be retained according to County retention schedules.

6.11 Remedial Training

Additional training may be required following policy violations, security incidents, or failed phishing exercises.

6.12 Annual Review

The Security Awareness & Training Program shall be reviewed at least annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.
- Approve major policy revisions.

7.2 County Leadership

- Support the Security Awareness Program.
- Ensure departmental participation.

7.3 Information Technology Director

- Administer the Security Awareness & Training Program.
- Approve training content.
- Ensure annual reviews and CJIS compliance.

7.4 Department Heads

- Ensure personnel complete required training.
- Monitor compliance.
- Notify IT of staffing changes affecting training.

7.5 Supervisors

- Verify employee participation.
- Address overdue training.
- Support remedial training when required.

7.6 Information Technology Staff

- Develop and deliver technical security training.
- Maintain training records.
- Coordinate phishing exercises where applicable.

7.7 Terminal Agency Coordinator (TAC)

- Identify and communicate CJIS training and testing requirements.
- Coordinate annual CJIS training and testing with Information Technology.
- Support CJIS audits and compliance reviews involving training records.

7.8 Users

- Complete required training on time.
- Apply training in daily work.
- Report suspected security incidents and phishing attempts.

7.9 Contractors and Volunteers

- Complete required training before receiving access when applicable.
- Comply with all County security policies.

8. Operational Procedures

8.1 New Personnel Training

1. Enroll new personnel in required security awareness training.
2. Complete general County training before or as soon as practical after system access is granted.
3. Complete required CJIS training and testing before CJI access is granted, when applicable.
4. Document completion.

8.2 Annual Refresher Training

1. Assign annual training, including required CJIS training and testing, to all applicable personnel.
2. Track completion status.
3. Follow up on overdue training.

8.3 Role-Based Training

1. Identify personnel requiring specialized training.
2. Provide role-based training before the related duties or CJI access begin and at least annually thereafter.
3. Maintain training records.

8.4 Phishing & Social Engineering

1. Conduct awareness activities and phishing simulations where appropriate.
2. Provide remedial training for users requiring additional education.

8.5 Incident Reporting Awareness

1. Train personnel to recognize suspicious activity.
2. Report suspected incidents through approved reporting channels.

8.6 Training Records

1. Maintain records of completed training.
2. Retain individual CJIS training records for at least three (3) years and retain other training records in accordance with County retention schedules.

8.7 Annual Program Review

1. Review training content.
2. Evaluate program effectiveness.
3. Document improvements.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, training records, and authorized audits.

- Required training shall be completed within established timeframes.
- Training records shall be maintained and available for audit.
- Personnel who fail to complete required training may have system access restricted until training is completed.
- Violations of this policy may result in disciplinary action.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJJ or a system used to process, store, or transmit CJJ shall be coordinated with the TAC

and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Training completion records
- Training attendance rosters
- CJIS Security Awareness training records
- Role-based training records
- Policy acknowledgement forms
- Phishing simulation results
- Remedial training documentation
- Annual program review documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0 — AT-2, AT-3, and AT-4
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 — AT-2, AT-3, and AT-4
- Morgan County MCIT-001 through MCIT-015 policies (Complete Policy, Table of Contents, page 1)

13. Revision History

Version	Date	Author	Description
2.0	September 2025	Information Technology Director	CJIS-compliant predecessor policy
3.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

New Employee Training Checklist

Complete	Task
☐	Training assigned
☐	Security policies acknowledged
☐	CJIS training and testing completed before CJI access, if applicable
☐	Completion documented

Annual Training Checklist

Complete	Task
☐	Annual training assigned
☐	Training completed
☐	Completion recorded
☐	Overdue users followed up

Role-Based Training Checklist

Complete	Task
☐	Role identified
☐	Specialized training completed
☐	Training documented

Phishing & Awareness Checklist

Complete	Task
☐	Awareness campaign completed
☐	Phishing exercise conducted
☐	Remedial training assigned if needed

Annual Program Review Checklist

Complete	Task
☐	Training content reviewed
☐	Training records audited
☐	Program effectiveness evaluated
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain individual CJIS training records for at least three (3) years. Maintain other training records, attendance rosters, policy acknowledgements, phishing exercise results, remedial training records, and annual program reviews in accordance with County retention schedules and applicable requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
FBI CJIS v6.0 AT-2 Literacy Training and Awareness	6.4; 8.1–8.2
NIST AT-2 Literacy & Awareness Training	6.1–6.2, 8.1–8.2
NIST AT-3 Role-Based Training	6.3, 8.3
NIST AT-4 Training Records	6.10, 8.6
NIST AT-2(3) Social Engineering and Mining	6.6, 8.4
NIST IR-6 Incident Reporting Awareness	6.7, 8.5
FBI CJIS v6.0 AT-3 Role-Based Training	6.3, 8.3
FBI CJIS v6.0 AT-4 Training Records	6.10, 8.6

Morgan County Personnel Security Policy & Procedures

Document Number: MCIT-002

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Personnel Security Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

The purpose of this Personnel Security Policy is to establish administrative, technical, and procedural safeguards to ensure only trustworthy and authorized individuals receive access to Morgan County information systems, Criminal Justice Information (CJI), Personally Identifiable Information (PII), and other sensitive County resources.

2. Authority

This policy supports compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy v6.0, Utah Department of Public Safety (DPS) requirements, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Personnel Security controls, Utah Government Records Access and Management Act (GRAMA), the Utah Government Data Privacy Act, and the Morgan County Information Security Program.

3. Scope

This policy applies to elected officials, employees, contractors, vendors, interns, volunteers, temporary personnel, managed service providers, and any individual granted physical or logical access to County systems, facilities, or information.

4. Objectives

Objectives include ensuring appropriate personnel screening, least privilege, timely removal of access, protection of CJI and PII, compliance with audit requirements, and consistent personnel security practices across all County departments.

5. Definitions

Key terms used in this policy include Access Authorization, CJI, Least Privilege, Privileged Account, Personnel Security, and Separation. These definitions establish a common understanding for all County personnel.

6. Personnel Security Policy

This section establishes the mandatory personnel security requirements for all Morgan County departments. Unless an approved exception exists, these requirements apply to every person granted physical or logical access to County information systems or facilities.

6.1 Personnel Screening

Individuals shall complete all required pre-employment screening before access to County systems is granted. Screening requirements shall be appropriate for the position and level of access.

6.2 Identity Verification

Identity shall be verified using government-issued identification and applicable employment verification procedures.

6.3 Background Investigations

Personnel requiring access to CJI shall complete all fingerprint-based state and national background investigations required by CJIS and Utah DPS.

6.4 Employment Eligibility

Access shall not be granted until employment eligibility and required screening activities have been completed.

6.5 Confidentiality and CJIS Access Agreements

Employees, contractors, and other authorized users shall acknowledge their responsibility to protect County information and comply with County security policies. Before receiving CJI access, each applicable user shall sign all individual CJIS security, access, training, and testing agreements or acknowledgments required by the State of Utah or other applicable CJIS authority. CJIS access agreements shall be reviewed at least annually and re-signed when required, when the agreement is updated, or when signatories change.

6.6 Security Awareness

Personnel shall complete security awareness training in accordance with MCIT-001 (Complete Policy, page 3). Personnel requiring CJI access shall complete applicable CJIS training and testing before receiving CJI access and at least annually thereafter.

6.7 Least Privilege

Access shall be limited to the minimum permissions necessary to perform assigned job duties.

6.8 Separation of Duties

Where practical, critical business functions shall be separated to reduce the risk of fraud, misuse, or unauthorized activity.

6.9 Access Approval

Department Heads and system owners shall approve access requests before accounts are created.

6.10 Annual Access Review

User access shall be reviewed at least annually, and more frequently for systems containing CJI or other sensitive information.

6.11 Personnel Transfers

Access rights shall be reviewed whenever job duties change. Unneeded access shall be removed before new privileges are assigned.

6.12 Emergency Termination

When immediate removal of access is necessary, IT shall disable accounts as soon as directed by authorized management.

6.13 Contractor Security

Contractors shall receive only the minimum access necessary and comply with all applicable County and CJIS requirements.

6.14 Privileged Administrators

Administrative privileges shall be granted only to authorized personnel with a documented business need.

6.15 Insider Threat Reporting

Personnel shall immediately report suspicious behavior, unauthorized access attempts, or suspected misuse of County information systems.

6.16 Policy and Procedure Review

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or CJIS systems, or changes to applicable laws, CJIS requirements, or NIST guidance.

6.17 Personnel Sanctions

Personnel who violate CJIS or County information security requirements are subject to sanctions consistent with County personnel policies and applicable law. Sanctions may include retraining, suspension or revocation of access, disciplinary action up to and including termination, referral for investigation or prosecution, and contract remedies. Sanctions shall be applied promptly, documented, and reported to the appropriate CJIS authority or authorities, as required, when misuse of CJI or CJIS systems is suspected or confirmed. When a formal sanctions process is initiated, designated internal information-security, personnel-security, and account-management officials shall be notified within twenty-four (24) hours.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight of the County information security program.
- Approve personnel security policies and significant revisions.
- Support resources necessary to implement this policy.

7.2 County Leadership

- Promote compliance with personnel security requirements.
- Support enforcement of disciplinary actions when warranted.

7.3 Human Resources

- Coordinate hiring, transfers, and separations with Information Technology.
- Ensure required background investigations are initiated.
- Notify IT immediately of employment status changes.
- Maintain personnel records in accordance with retention requirements.

7.4 Department Heads

- Approve access requests based on business need.
- Review user access at least annually.
- Notify IT immediately when access should be changed or removed.
- Ensure personnel complete required training.

7.5 Information Technology Director

- Administer the Personnel Security Program.
- Approve privileged access requests.
- Ensure compliance with CJIS personnel security requirements.
- Coordinate periodic audits and policy reviews.

7.6 Terminal Agency Coordinator (TAC)

- Ensure personnel with CJ access meet CJIS requirements.
- Coordinate with the Local Agency Security Officer (LASO) and support CJIS audits and compliance reviews.
- Maintain current CJIS agency agreements, Originating Agency Identifier (ORI) validations, and individual user agreements. Notify IT of annual CJIS training and testing requirements; IT retains records under MCIT-001 (Complete Policy, page 4).

7.7 Local Agency Security Officer (LASO)

- Verify fingerprint-based background checks when required.
- Monitor ongoing CJS compliance.
- Maintain documentation supporting personnel security controls.

7.8 Information Technology Staff

- Provide and remove accounts.
- Implement least privilege.
- Maintain authentication systems and audit records.
- Assist with investigations involving personnel access.

7.9 System Owners

- Approve application-specific permissions.
- Participate in periodic access reviews.
- Validate that users retain a business need for access.

7.10 Supervisors

- Monitor employee compliance with security requirements.
- Report suspected insider threats or policy violations.
- Ensure departing personnel surrender County assets.

7.11 Employees

- Protect County information and credentials.
- Complete required training.
- Report lost devices, badges, or suspected security incidents immediately.
- Comply with all County security policies.

7.12 Contractors and Third Parties

- Comply with applicable County policies and contractual security requirements.
- Use County information only for authorized purposes.
- Return County credentials, devices, media, records, and information at contract completion, or securely destroy County information and media as specifically directed by Morgan County. Destruction shall be documented where required and shall not occur while an applicable retention requirement, legal hold, audit, litigation matter, public-records request, or other preservation obligation remains in effect.

8. Operational Procedures

8.1 New Hire / Onboarding

1. Human Resources notifies Information Technology of the pending hire.
2. Department Head submits an access request identifying required systems.
3. Identity and employment eligibility are verified.
4. Required background investigations and fingerprint checks are completed when applicable.
5. Required confidentiality agreements are signed.
6. Required CJIS security, access, training, and testing agreements or acknowledgments are signed before CJI access, when applicable.
7. Required security awareness training is assigned; applicable CJIS training and testing are completed before CJI access.
8. IT creates user accounts using least privilege.
9. MFA is configured and verified on every County-owned computer and for all privileged and non-privileged user accounts.
10. Equipment is assigned and inventoried.
11. Manager confirms access is appropriate on the employee's first day.

8.2 Access Authorization

1. Each access request must identify a business need.
2. Department Head approves requested access.
3. System Owner approves application-specific access where applicable.
4. IT documents account creation and assigned permissions.

8.3 Personnel Transfers

1. Supervisor notifies HR and IT of the position change.
2. Existing permissions are reviewed.
3. Unnecessary access is removed.

4. New permissions are approved before assignment.
5. Privileged access is revalidated.

8.4 Annual Access Review

1. IT exports active user accounts.
2. Department Heads review personnel access.
3. Inactive or unnecessary accounts are removed.
4. Review results are documented and retained.

8.5 Privileged User Administration

1. Administrative accounts shall be separate from standard user accounts whenever practical.
2. Privileged access shall be reviewed more frequently than standard accounts.
3. Shared administrator accounts are prohibited unless formally approved and documented.

8.6 Contractor Management

1. Contract requirements are verified.
2. Security agreements are completed when required.
3. Temporary accounts receive expiration dates.
4. Access is removed immediately upon contract completion.
5. County credentials, devices, media, records, and information are returned at contract completion, or County information and media are securely destroyed as specifically directed by Morgan County. Destruction is documented where required and does not occur while an applicable retention requirement, legal hold, audit, litigation matter, public-records request, or other preservation obligation remains in effect.

8.7 Employee Separation

1. HR immediately notifies IT.
2. User accounts are disabled.
3. VPN, MFA, badges, keys, and remote access are revoked.

4. County equipment is recovered by the deadline stated in the request or, if no deadline is stated, within two County business days. Information Technology may require same-day return when continued possession presents a documented security or operational risk, coordinated with Human Resources and the applicable Department Head, Director, or Elected Official.
5. Completion is documented.

8.8 Emergency Termination

1. Authorized management may direct immediate account disablement.
2. IT disables logical access without delay.
3. Physical access credentials are revoked.
4. Evidence is preserved if misconduct is suspected.

8.9 Personnel Sanctions

1. Supervisors, Information Technology, or other personnel report suspected misuse or policy violations to authorized management and Human Resources.
2. Information Technology preserves relevant evidence and suspends or limits access immediately when continued access presents a security risk.
3. Human Resources and authorized management determine and apply sanctions consistent with County policy, contracts, and applicable law.
4. When a formal sanctions process is initiated, Information Technology, Human Resources, account-management personnel, and other designated internal security officials are notified within twenty-four (24) hours.
5. The TAC or designated organizational personnel with security responsibilities reports CJI or CJS-system misuse to the appropriate CJS authority or authorities, as required.
6. The investigation, access action, sanction, and required external reporting are documented and retained.

8.10 Documentation

1. Personnel security records shall be retained according to County retention schedules.
2. Background investigation records shall be protected as confidential.
3. Access approvals and review records shall be maintained for audit purposes.

9. Compliance

Morgan County shall periodically review compliance with this policy through internal reviews, management oversight, and external audits. Personnel security controls shall be evaluated to ensure they remain effective and continue to meet operational, legal, and CJIS requirements.

- Non-compliance may result in suspension or revocation of system access.
- Policy violations may result in disciplinary action up to and including termination.
- Criminal violations may be referred to the appropriate law enforcement agency.
- Contractors may have contracts suspended or terminated for non-compliance.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJ or a system used to process, store, or transmit CJ shall be coordinated with the TAC and LASO and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

The following documentation should be retained as evidence that this policy is being implemented:

- Completed background investigation documentation
- CJIS fingerprint verification records
- Signed confidentiality agreements
- Signed individual CJIS security, access, training, and testing agreements or acknowledgments
- Security awareness training completion reports
- Access request approvals
- Quarterly or annual access review records
- Employee onboarding checklists
- Employee transfer documentation
- Employee separation checklists
- Contractor onboarding and offboarding records
- Privileged account review reports
- Active Directory account creation and disablement records
- Personnel sanction and CJ misuse-reporting records
- Twenty-four-hour sanctions-process notification records, when applicable

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0 — CA-3, AT-2 through AT-4, PS-6, and PS-8
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 — CA-3, AT-2 through AT-4, PS-6, and PS-8
- NIST Special Publication 800-61 Revision 2
- Utah Department of Public Safety CJIS Requirements
- Utah Government Records Access and Management Act (GRAMA)
- Utah Government Data Privacy Act
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)
- Morgan County Identification & Authentication Policy (MCIT-009; Complete Policy, page 82)
- Morgan County Security Awareness & Training Policy (MCIT-001; Complete Policy, page 2)
- Morgan County Incident Response Plan (MCIT-008; Complete Policy, page 74)

13. Revision History

Version	Date	Author	Description
1.0	2025	Morgan County	Predecessor Discipline and Misuse policy used for the 2025 CJIS audit
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; contractor disposition and equipment-return procedures updated; pending approval

Appendices, Forms & Checklists

Appendix A – New Hire Checklist

New Employee Onboarding

Complete	Task
☐	Offer accepted
☐	Identity verified
☐	Employment eligibility verified
☐	Background investigation completed (if required)
☐	CJIS fingerprint results received (if applicable)
☐	Confidentiality agreement signed

Complete	Task
☐	Required CJIS agreements signed, if applicable
☐	Security training assigned; CJIS training/testing completed before CJI access, if applicable
☐	User account created
☐	MFA configured and verified
☐	Least privilege applied
☐	Equipment assigned and documented
☐	Manager verified required access

Appendix B – Personnel Transfer Checklist

Transfer Review

Complete	Task
☐	Supervisor notified HR and IT
☐	Existing permissions reviewed
☐	Unneeded permissions removed
☐	New permissions approved
☐	Privileged access revalidated
☐	Documentation updated

Appendix C – Employee Separation Checklist

Termination / Separation

Complete	Task
☐	HR notified IT
☐	User account disabled
☐	VPN disabled
☐	MFA revoked
☐	Email access removed
☐	Administrative privileges removed
☐	Keys recovered
☐	Badge recovered
☐	County equipment returned
☐	Documentation retained

Appendix D – Contractor Administration

Contractor Onboarding

Complete	Task
☐	Contract approved
☐	Business need verified
☐	Security agreement completed
☐	CJIS Security Addendum or MCA completed if applicable
☐	Temporary account created
☐	Account expiration date established

Contractor Offboarding

Complete	Task
☐	Contract completed
☐	Account disabled
☐	VPN removed
☐	Equipment returned
☐	Badge and keys recovered
☐	Access records updated

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
FBI CJIS v6.0 CA-3 Information Exchange	6.5, 7.6, 8.1
NIST PS-3 Personnel Screening	6.1–6.4, 8.1
NIST PS-4 Personnel Termination	6.12, 8.7–8.8
NIST PS-5 Personnel Transfer	6.11, 8.3
NIST PS-7 External Personnel Security	6.13, 8.6
NIST PS-8 Personnel Sanctions	6.17, 8.9, 9
FBI CJIS v6.0 PS-6 Access Agreements	6.5, 8.1
FBI CJIS v6.0 PS-8 Personnel Sanctions	6.17, 8.9
NIST CA-3 Information Exchange	6.5, 7.6, 8.1
NIST PS-6 Access Agreements	6.5, 8.1

Morgan County Access Control Policy & Procedures

Document Number: MCIT-003

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Access Control Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

This policy establishes the requirements for granting, managing, reviewing, and revoking logical and physical access to Morgan County information systems and information assets in accordance with business need, least privilege, and Criminal Justice Information Services (CJIS) requirements.

2. Authority

This policy supports the FBI CJIS Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Access Control (AC) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County-owned or managed information systems, cloud services, applications, network devices, workstations, mobile devices, physical access systems, and users including employees, contractors, vendors, volunteers, and temporary personnel.

4. Objectives

Ensure only authorized users receive access, enforce least privilege and need-to-know, require management approval, perform periodic access reviews, and promptly remove unnecessary access.

5. Definitions

Key terms include Access Control, Least Privilege, Need-to-Know, Role-Based Access Control (RBAC), Privileged Account, Physical Access, and Logical Access.

6. Access Control Policy

The following requirements establish the minimum access control requirements for Morgan County information systems. These requirements apply to all production systems unless an approved exception exists.

6.1 Access Authorization

Access shall be granted only after documented management approval and verification of a legitimate business need.

6.2 Least Privilege

Users shall receive only the minimum permissions necessary to perform assigned job duties.

6.3 Need-to-Know

Access to sensitive information shall be limited to individuals with an authorized need-to-know.

6.4 Role-Based Access Control (RBAC)

Where practical, access shall be assigned through defined security roles rather than individual permissions.

6.5 Physical Access

Physical access to information systems and restricted areas shall be limited to authorized personnel.

6.6 Remote Access

Remote access shall use approved secure technologies and multi-factor authentication (MFA). MFA is required for all County-owned computers and for privileged and non-privileged accounts.

6.7 Privileged Access

Administrative privileges shall be limited, documented, periodically reviewed, and monitored.

6.8 Temporary Access

Temporary and emergency accounts shall have an approved expiration date and shall be automatically disabled or removed within seventy-two (72) hours unless a shorter approved period applies.

6.9 Third-Party Access

Vendor and contractor access shall be approved, documented, monitored, and removed upon completion of work.

6.10 Session Locking

Systems shall automatically lock inactive sessions where technically feasible.

6.11 Network Access

Access to internal networks shall be restricted using approved security controls including firewalls, VPNs, and network segmentation where appropriate.

6.12 Wireless Access

Wireless access shall use approved encryption and authentication mechanisms.

6.13 Periodic Access Reviews

Department Heads and System Owners shall review user access at least annually.

6.14 Account Disablement and Access Revocation

Accounts shall be disabled immediately upon involuntary termination or when continued access presents an unacceptable risk. Expired accounts, accounts no longer associated with a user, accounts in violation of policy, and accounts inactive for ninety (90) calendar days shall be disabled within one (1) week. Accounts of individuals identified as a direct threat to the confidentiality, integrity, or availability of Criminal Justice Information (CJI) shall be disabled within thirty (30) minutes of discovery.

6.15 Annual Review

The Access Control Program shall be reviewed annually and after significant technology or organizational changes.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.
- Approve major policy revisions.

7.2 County Leadership

- Support implementation and compliance.
- Ensure departments follow access control requirements.

7.3 Information Technology Director

- Administer the Access Control Program.
- Approve privileged access standards.
- Ensure annual access reviews are completed.

7.4 Department Heads

- Approve access requests.
- Review user access annually.
- Notify IT of staffing changes.

7.5 System Owners

- Approve application-specific access.
- Validate access requirements.

- Participate in periodic reviews.

7.6 Information Technology Staff

- Provide and remove accounts.
- Implement least privilege.
- Manage remote access and MFA.
- Maintain access records.

7.7 Supervisors

- Ensure users follow access control requirements.
- Report inappropriate access.

7.8 Users

- Use only authorized accounts.
- Protect credentials.
- Report suspected unauthorized access.

7.9 Contractors

- Use only approved accounts.
- Comply with County access requirements.
- Return County credentials, devices, media, records, and information at contract completion, or securely destroy County information and media as specifically directed by Morgan County. Destruction shall be documented where required and shall not occur while an applicable retention requirement, legal hold, audit, litigation matter, public-records request, or other preservation obligation remains in effect.

8. Operational Procedures

8.1 Access Request

1. Department Head submits an access request.
2. Business need is verified.
3. Required approvals are obtained.
4. Information Technology Staff provides access using least privilege.

8.2 Access Modification

1. Review requested changes.
2. Remove unnecessary access.
3. Document significant changes.

8.3 Privileged Access

1. Approve privileged access separately.
2. Maintain separate administrative accounts where practical.
3. Review privileged access periodically.

8.4 Temporary Access

1. Assign expiration dates.
2. Review before extension.
3. Automatically disable or remove temporary and emergency accounts within seventy-two (72) hours.

8.5 Third-Party Access

1. Verify contractual authorization.
2. Limit access to required resources.
3. Disable access when work is complete.

8.6 Remote Access

1. Require approved VPN or equivalent.
2. Require MFA.
3. Monitor remote access activity.

8.7 Periodic Access Reviews

1. Review user access at least annually.
2. Remove unnecessary permissions.

3. Document review results.

8.8 Access Revocation

1. Disable accounts immediately upon involuntary termination or when continued access presents an unacceptable risk.
2. Within one (1) week, disable expired accounts, accounts no longer associated with a user, accounts in violation of policy, and accounts inactive for ninety (90) calendar days.
3. Disable direct-threat individual accounts within thirty (30) minutes of discovery and remove associated VPN, badge, MFA, and privileged access.
4. Document the disablement, revocation time, responsible personnel, and completion evidence.

8.9 Annual Program Review

1. Review access control standards.
2. Review privileged access.
3. Document corrective actions.

9. Compliance

Morgan County shall periodically review compliance with this policy through internal reviews, management oversight, and CJIS or other authorized audits.

- Access approvals shall be documented.
- Access reviews shall be completed at least annually.
- Unauthorized access shall be investigated.
- Violations may result in disciplinary action or removal of access.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJJ or a system used to process, store, or transmit CJJ shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Access request forms
- Management approvals
- Privileged account reviews
- Annual access review reports
- Temporary access records
- Remote access logs
- Account disablement records
- Corrective action documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Access Control (AC)
- Morgan County Personnel Security Policy (MCIT-002; Complete Policy, page 11)
- Morgan County Identification & Authentication Policy (MCIT-009; Complete Policy, page 82)
- Morgan County Audit & Accountability Policy (MCIT-011; Complete Policy, page 104)

13. Revision History

Version	Date	Author	Description
1.0	09/15/2023	Jeremy Archibald	Initial draft
1.1	09/03/2024	Jeremy Archibald	Reviewed; adopted 8/19/2025 (CR 25-39)
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; contractor return and secure-destruction requirements updated; pending approval

Appendices, Forms & Checklists

Access Request Checklist

Complete	Task
☐	Business needs documented
☐	Department Head approval received
☐	Least privilege applied
☐	System Owner approval obtained if required

Complete	Task
☐	Access provisioned
☐	Request documented

Privileged Access Review

Complete	Task
☐	Business need verified
☐	Administrative rights validated
☐	Inactive privileged accounts removed
☐	Review documented

Temporary / Third-Party Access

Complete	Task
☐	Expiration date assigned
☐	Sponsor identified
☐	Access reviewed
☐	Access removed when complete

Account Revocation

Complete	Task
☐	Account disabled
☐	VPN revoked
☐	MFA revoked
☐	Badge/physical access removed
☐	Completion documented

Annual Access Review

Complete	Task
☐	User access reviewed
☐	Role assignments validated
☐	Least privilege verified
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain access requests, approvals, review records, privileged access reviews, remote access logs, and account revocation records in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies,

records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.



Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Access Control	Sections 6–8
NIST AC-2 Account Management, including AC-2(2), AC-2(3), and AC-2(13)	6.1, 6.8, 6.14; 8.1, 8.4, 8.8
NIST AC-3 Access Enforcement	6.2–6.4
NIST AC-6 Least Privilege	6.2, 6.7
NIST AC-17 Remote Access	6.6, 8.6



Morgan County Personally Identifiable Information (PII) Protection Policy & Procedures

Document Number: MCIT-004

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. PII Protection Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements for collecting, accessing, storing, transmitting, sharing, retaining, and disposing of Personally Identifiable Information (PII) to protect the privacy of individuals and comply with applicable legal and regulatory requirements.

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Privacy and Security controls, Utah Government Data Privacy Act, Utah Government Records Access and Management Act (GRAMA), and Morgan County information security policies.

3. Scope

Applies to all County departments, employees, contractors, volunteers, systems, cloud services, paper records, and electronic records containing PII.

4. Objectives

Protect PII from unauthorized access, disclosure, alteration, or destruction while ensuring lawful collection, use, retention, and disposal.

5. Definitions

Key terms include PII, Sensitive PII, Data Owner, Data Custodian, Disclosure, and Minimum Necessary.

6. PII Protection Policy

The following requirements establish the minimum protections for PII maintained by Morgan County.

6.1 Lawful Collection

PII shall be collected only for authorized governmental purposes and limited to the minimum information necessary.

6.2 Classification

PII shall be classified and handled according to its sensitivity and applicable legal requirements.

6.3 Access Control

Access to PII shall be restricted to authorized personnel with a documented business need.

6.4 Use and Disclosure

PII shall only be used or disclosed for authorized purposes and in accordance with applicable laws and County policy. Before releasing reports, discovery, records, or other materials, personnel shall review the material for PII and redact information that is not authorized or required for the disclosure. Required discovery and court-ordered disclosures shall be handled in accordance with applicable law, court rules, court orders, and County Attorney procedures. Discovery containing Criminal Justice Information (CJI) shall be disseminated only through eProsecutor to authorized recipients.

6.5 Storage

PII shall be stored using approved physical and electronic safeguards.

6.6 Transmission

PII transmitted electronically shall use an approved secure method and encryption where required by applicable law, policy, or risk.

6.7 Retention

PII shall be retained in accordance with approved records retention schedules.

6.8 Disposal

PII shall be securely destroyed when no longer required.

6.9 Incident Reporting

Suspected unauthorized disclosure or compromise of PII shall be reported immediately.

6.10 Third-Party Access

Third parties handling County PII shall provide appropriate contractual and security protections.

6.11 Privacy Reviews

New systems, procurements, programs, and significant changes that process PII shall undergo a documented privacy impact assessment before implementation when required by law or County risk determination. The assessment shall be updated when changes alter privacy risk.

6.12 Annual Review

The PII Protection Program shall be reviewed annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.

- Approve major policy revisions.

7.2 County Leadership

- Support privacy compliance.
- Ensure departmental adherence to this policy.

7.3 Information Technology Director

- Administer the PII Protection Program.
- Implement technical safeguards.
- Coordinate breach response involving electronic records.

7.4 Department Heads

- Approve access to PII.
- Ensure staff handle PII appropriately.
- Report suspected privacy incidents promptly.

7.5 Data Owners

- Classify PII.
- Approve access based on business need.
- Review access periodically.

7.6 Information Technology Staff

- Implement security controls.
- Protect electronic PII.
- Maintain encryption, backups, and logging where applicable.

7.7 Supervisors

- Ensure employees comply with PII handling requirements.
- Report suspected violations.

7.8 Users

- Access PII only for authorized purposes.
- Protect PII from unauthorized disclosure.
- Report suspected compromises immediately.

7.9 Contractors

- Comply with County privacy requirements.
- Protect County PII.
- Return PII at contract completion or securely destroy it as specifically directed by Morgan County. Destruction shall be documented where required and shall not occur while an applicable retention requirement, legal hold, audit, litigation matter, public-records request, or other preservation obligation remains in effect.

8. Operational Procedures

8.1 PII Collection

1. Collect only the minimum PII necessary for the authorized purpose.
2. Provide required notices when applicable.
3. Document the business purpose for collection.

8.2 Access to PII

1. Verify a legitimate business need before granting access.
2. Apply least privilege.
3. Review access periodically.

8.3 Storage and Transmission

1. Store PII only in approved locations.
2. Encrypt PII during transmission where required.
3. Protect physical records from unauthorized access.

8.4 Disclosure

1. Verify authorization before releasing PII.
2. Disclose only the minimum necessary information.
3. Document disclosures when required by law or policy.
4. Review reports, discovery, records, and other materials for PII and redact information that is not authorized or required for disclosure.

5. Verify applicable discovery requirements, court rules, court orders, and County Attorney procedures before release.
6. Transmit materials containing PII using an approved secure method.
7. Disseminate discovery containing CJI only through eProsecutor to an authorized recipient.

8.5 Retention and Disposal

1. Retain records according to approved retention schedules.
2. Securely destroy paper and electronic PII when authorized.

8.6 Privacy Incident Response

1. Immediately report suspected PII exposure.
2. Contain the incident.
3. Preserve evidence.
4. Coordinate notification requirements with County leadership.

8.7 Annual Privacy Review

1. Review PII inventories.
2. Review access controls.
3. Document corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, privacy assessments, and authorized audits.

- PII shall be accessed only by authorized personnel.
- PII handling shall comply with applicable laws, regulations, and County policy.
- Privacy incidents shall be investigated and documented.
- Violations of this policy may result in disciplinary action.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and

compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- PII access approval records
- PII inventory records
- Privacy assessment documentation
- PII disclosure records
- PII redaction-review records, when required
- Discovery disclosure, eProsecutor dissemination, and secure-transmission records, when required
- Records retention documentation
- Secure destruction records
- Privacy incident reports
- Annual privacy review reports
- Corrective action documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Privacy and Security Controls
- Utah Government Data Privacy Act
- GRAMA, including Utah Code § 63G-2-207
- Utah Rules of Criminal Procedure, Rule 16 (Discovery)
- Utah Code § 77-38-6 (Victim privacy)
- Morgan County Incident Response Policy (MCIT-008; Complete Policy, page 74)
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)

13. Revision History

Version	Date	Author	Description
1.0	May 1, 2024	Jeremy Archibald	Initial release
1.1	Sept. 16, 2024	Jeremy Archibald	Expanded PII policy; adopted 8/19/2025 (CR 25-43)

Version	Date	Author	Description
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; contractor and records-disposition safeguards updated; pending approval

Appendices, Forms & Checklists

PII Collection Checklist

Complete	Task
☐	Business purpose documented
☐	Minimum necessary information collected
☐	Required notice provided
☐	Collection approved where required

PII Access Review Checklist

Complete	Task
☐	Business need verified
☐	Least privilege confirmed
☐	Access approvals current
☐	Review documented

PII Disclosure Checklist

Complete	Task
☐	Disclosure authorized
☐	Minimum necessary disclosed
☐	Disclosure documented
☐	Recipient verified
☐	PII and redaction review completed, when applicable
☐	Discovery, court-rule, court-order, and County Attorney requirements verified
☐	Approved secure transmission method used
☐	Discovery containing CJI disseminated only through eProsecutor

Secure Disposal Checklist

Complete	Task
☐	Retention period satisfied

Complete	Task
☐	Paper records shredded
☐	Electronic media sanitized
☐	Disposal documented



Annual Privacy Review Checklist

Complete	Task
☐	PII inventory reviewed
☐	Access reviewed
☐	Privacy incidents reviewed
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain PII inventories, access approvals, disclosure records, privacy assessments, incident reports, destruction records, and annual review documentation in accordance with County retention schedules and applicable legal requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS, NIST & Legal Control Mapping

Control	Policy Section
CJIS Privacy Requirements	Sections 6–8
NIST PT-2 Authority to Process PII	6.1, 6.4; 8.1–8.2
NIST RA-8 Privacy Impact Assessments	6.11, 8.7
NIST SI-12(1) Limit PII Elements	6.1, 8.1
NIST MP-6 Media Sanitization	6.8, 8.5
NIST PT-3 PII Processing Purposes	6.1, 6.4; 8.1–8.2
Utah R. Crim. P. 16 — Discovery	6.4, 8.4
Utah Code § 63G-2-207 — Protected and private records in discovery	6.4, 8.4
Utah Code § 77-38-6 — Victim privacy	6.4, 8.4

Morgan County Media Protection Policy & Procedures

Document Number: MCIT-005

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Media Protection Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements for protecting paper and electronic media containing County information throughout its lifecycle, including storage, transport, reuse, and disposal.

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Media Protection (MP) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County-owned or managed electronic media, removable media, printed records, backup media, and storage devices containing County information.

4. Objectives

Protect media from unauthorized access, disclosure, alteration, theft, loss, and improper disposal.

5. Definitions

Key terms include Media, Removable Media, Sanitization, Destruction, Backup Media, and Chain of Custody.

6. Media Protection Policy

The following requirements establish the minimum media protection requirements for Morgan County information systems and information assets.

6.1 Media Classification

Media shall be handled according to the sensitivity of the information it contains.

6.2 Media Access

Access to media containing County information shall be limited to authorized personnel.

6.3 Media Storage

Media shall be stored in secure locations that protect against unauthorized access, damage, and environmental hazards.

6.4 Media Transport

Media transported outside County facilities shall be protected from loss, theft, and unauthorized disclosure.

6.5 Removable Media

Use of removable media shall be limited to authorized business purposes and County-approved devices. Personally owned removable media is prohibited. Removable media containing CJI or other sensitive County information shall be authorized by Information Technology and protected with approved encryption.

6.6 Media Reuse

Media shall be sanitized before reuse when previously used to store sensitive information.

6.7 Media Disposal

Paper and electronic media shall be securely destroyed or sanitized before disposal.

6.8 Backup Media

Backup media shall be protected, inventoried, and stored securely.

6.9 Chain of Custody

Chain of custody shall be maintained when required for sensitive or evidentiary media.

6.10 Third-Party Handling

Third parties handling County media shall comply with contractual security requirements.

6.11 Lost or Stolen Media

Lost or stolen media shall be reported immediately and investigated.

6.12 Annual Review

The Media Protection Program shall be reviewed at least annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.
- Approve major policy revisions.

7.2 County Leadership

- Support implementation of media protection controls.
- Ensure departmental compliance.

7.3 Information Technology Director

- Administer the Media Protection Program.
- Approve media handling standards.
- Ensure annual reviews are completed.

7.4 Department Heads

- Ensure media containing County information is protected.
- Approve media removal when required.
- Report lost or stolen media immediately.

7.5 Data Owners

- Classify information stored on media.
- Approve access based on business need.
- Review handling requirements periodically.

7.6 Information Technology Staff

- Manage secure storage, transport, sanitization, and disposal of electronic media.
- Maintain backup media protections.
- Document media destruction.

7.7 Supervisors

- Ensure employees follow media protection requirements.
- Report suspected policy violations.

7.8 Users

- Protect media in their custody.
- Use removable media only as authorized.
- Report lost or stolen media immediately.

7.9 Contractors

- Protect County media.
- Comply with contractual media handling requirements.
- Return County media at contract completion or securely destroy it as specifically directed by Morgan County. Destruction shall be documented where required and shall not occur while an applicable retention requirement, legal hold, audit, litigation matter, public-records request, or other preservation obligation remains in effect.

8. Operational Procedures

8.1 Media Classification

1. Classify media based on the sensitivity of the information it contains.
2. Apply appropriate handling requirements.

8.2 Media Storage

1. Store media in secure locations.
2. Protect media from unauthorized access, theft, damage, and environmental hazards.

8.3 Media Transport

1. Authorize transport of sensitive media.
2. Use appropriate protective containers and safeguards.
3. Maintain chain of custody when required.

8.4 Removable Media

1. Use only County-approved removable media for an authorized business purpose; personally owned removable media is prohibited.
2. Obtain Information Technology authorization and use approved encryption before storing CJI or other sensitive County information on removable media.
3. Scan removable media for malicious code before use and maintain physical control of the media while CJI or sensitive County information is present.

8.5 Media Sanitization & Disposal

1. Sanitize electronic media before reuse.
2. Destroy media using approved methods before disposal.
3. Document destruction where required.

8.6 Lost or Stolen Media

1. Immediately report lost or stolen media.

2. Investigate the incident.
3. Take corrective actions as appropriate.

8.7 Annual Media Review

1. Review media inventories.
2. Review storage and disposal procedures.
3. Document corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, and authorized audits.

- Media shall be protected according to its classification.
- Approved sanitization and destruction methods shall be used.
- Lost or stolen media shall be reported immediately.
- Violations may result in disciplinary action.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Media inventories
- Backup media inventories
- Media transport records
- Chain of custody records
- Media sanitization records
- Media destruction certificates
- Lost or stolen media reports
- Annual media review documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Media Protection (MP)
- National Institute of Standards and Technology (NIST) NIST SP 800-88 Rev. 1 Media Sanitization
- Morgan County PII Protection Policy (MCIT-004; Complete Policy, page 35)
- Morgan County Incident Response Policy (MCIT-008; Complete Policy, page 74)

13. Revision History

Version	Date	Author	Description
1.0	August 2025	Morgan County	Legacy media policies; predecessor v1.0 designation
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; contractor and records-disposition safeguards updated; pending approval

Appendices, Forms & Checklists

Media Inventory Checklist

Complete	Task
☐	Media identified
☐	Owner assigned
☐	Classification verified
☐	Inventory updated

Media Transport Checklist

Complete	Task
☐	Transport authorized
☐	Container secured
☐	Chain of custody documented if required
☐	Delivery confirmed

Removable Media Checklist

Complete	Task
☐	Approved device used

Complete	Task
☐	Encrypted if required
☐	Malware scan completed
☐	Business need documented

Media Sanitization & Disposal Checklist

Complete	Task
☐	Retention period satisfied
☐	Approved sanitization method used
☐	Media destroyed or sanitized
☐	Destruction documented

Annual Media Protection Review

Complete	Task
☐	Inventory reviewed
☐	Storage locations inspected
☐	Disposal records reviewed
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain media inventories, transport logs, chain of custody records, sanitization records, destruction certificates, and annual review documentation in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with Section 6.7 of this policy. Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Media Protection	Sections 6–8

Control	Policy Section
NIST MP-2 Media Access	6.2
NIST MP-4 Media Storage	6.3, 8.2
NIST MP-5 Media Transport	6.4, 8.3
NIST MP-6 Media Sanitization	6.6-6.7, 8.5
NIST MP-7 Media Use	6.5, 8.4



Morgan County Physical Protection Policy & Procedures

Document Number: MCIT-006

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Physical Protection Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements to protect County facilities, information systems, and personnel from unauthorized physical access, damage, theft, or disruption.

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Physical and Environmental Protection (PE) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County facilities, data rooms, communication closets, offices, equipment, visitors, contractors, and physical security systems.

4. Objectives

Protect facilities and equipment through controlled physical access, monitoring, visitor management, and environmental safeguards.

5. Definitions

Key terms include Controlled Area, Visitor, Badge, Escort, Physical Access Device, and Secure Area.

6. Physical Protection Policy

The following requirements establish the minimum physical protection requirements for Morgan County facilities, information systems, and assets.

6.1 Physical Access Authorization

Access to controlled areas shall be granted only to authorized individuals with a documented business need.

6.2 Controlled Areas

Server rooms, network closets, evidence storage, and other sensitive areas shall be physically secured.

6.3 Visitor Management

Visitors shall be authorized, logged, and escorted where required.

6.4 Physical Access Devices

Keys, badges, and access cards shall be issued, tracked, and promptly revoked when no longer required.

6.5 Monitoring

Controlled areas shall be monitored using appropriate security measures such as cameras, alarms, or access logs where practical.

6.6 Environmental Protection

Critical equipment shall be protected from fire, water, power disruption, and environmental hazards.

6.7 Equipment Protection

County equipment shall be secured against theft, tampering, or unauthorized removal.

6.8 Deliveries

Deliveries to controlled areas shall be monitored and restricted.

6.9 Emergency Access

Emergency responders may be granted access as necessary while maintaining security whenever practical.

6.10 Lost Access Devices

Lost or stolen keys, badges, or access cards shall be reported immediately.

6.11 Third-Party Access

Contractors and vendors shall be authorized, supervised, and limited to approved areas.

6.12 Annual Review

The Physical Protection Program shall be reviewed at least annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.
- Approve major policy revisions.

7.2 County Leadership

- Support implementation of physical security controls.
- Ensure departmental compliance.

7.3 Information Technology Director

- Administer the Physical Protection Program.
- Approve physical security standards.
- Coordinate protection of IT facilities.

- Ensure annual reviews are completed.

7.4 Department Heads

- Authorize physical access based on business need.
- Ensure employees follow physical security requirements.
- Report physical security incidents.

7.5 Facilities Management

- Maintain physical security systems.
- Coordinate building maintenance affecting secure areas.
- Support environmental controls.

7.6 Information Technology Staff

- Protect server rooms and network closets.
- Manage physical access to IT equipment.
- Maintain access records where applicable.

7.7 Supervisors

- Ensure employees comply with physical security procedures.
- Report lost access devices or suspicious activity.

7.8 Users

- Wear or present identification when required.
- Protect keys and access badges.
- Report lost credentials or security concerns immediately.

7.9 Contractors and Visitors

- Access only approved areas.
- Comply with escort requirements.
- Return temporary badges before departure.

8. Operational Procedures

8.1 Physical Access Requests

1. Verify business need.
2. Obtain required approvals.
3. Issue access device.
4. Document issuance.

8.2 Visitor Management

1. Verify visitor identity.
2. Record visitor in the visitor log.
3. Provide escort when required.
4. Collect visitor badge upon departure.

8.3 Controlled Areas

1. Keep controlled areas locked when unattended.
2. Limit access to authorized personnel.
3. Review access permissions periodically.

8.4 Equipment Protection

1. Secure IT equipment against theft or tampering.
2. Protect portable devices when unattended.

8.5 Environmental Controls

1. Maintain fire suppression where applicable.
2. Maintain temperature and humidity controls.
3. Protect against power interruptions.

8.6 Lost Access Devices

1. Report lost keys or badges immediately.
2. Disable electronic credentials promptly.
3. Rekey or replace locks when appropriate.

8.7 Annual Physical Security Review

1. Inspect controlled areas.
2. Review physical access lists.
3. Review visitor procedures.
4. Document corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, facility inspections, and authorized audits.

- Physical access shall be limited to authorized personnel.
- Visitors shall comply with visitor management procedures.
- Physical security incidents shall be documented and investigated.
- Violations may result in disciplinary action or revocation of physical access.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting Criminal Justice Information (CJI) or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Physical access authorization records
- Key and badge inventories
- Visitor logs
- Access control system reports
- Controlled area inspection records

- Environmental monitoring records
- Physical security incident reports
- Annual physical security review documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Physical and Environmental Protection (PE)
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)
- Morgan County Incident Response Policy (MCIT-008; Complete Policy, page 74)
- Morgan County Media Protection Policy (MCIT-005; Complete Policy, page 45)

13. Revision History

Version	Date	Author	Description
1.0	August 19, 2025	Morgan County	Legacy policy adopted (CR 25-42)
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

Physical Access Request Checklist

Complete	Task
☐	Business need verified
☐	Management approval obtained
☐	Access device issued
☐	Access documented

Visitor Management Checklist

Complete	Task
☐	Visitor identity verified
☐	Visitor logged
☐	Escort assigned if required
☐	Badge collected upon departure

Controlled Area Inspection Checklist

Complete	Task
☐	Doors secured
☐	Access lists reviewed
☐	Environmental controls operational
☐	Unauthorized items removed

Lost Access Device Checklist

Complete	Task
☐	Incident reported
☐	Credential disabled
☐	Locks or permissions updated if required
☐	Incident documented

Annual Physical Security Review Checklist

Complete	Task
☐	Controlled areas inspected
☐	Badge inventory reviewed
☐	Visitor logs reviewed
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain access authorization records, badge inventories, visitor logs, inspection reports, environmental monitoring records, physical security incident reports, and annual review documentation in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Physical Protection	Sections 6–8
NIST PE-2 Physical Access Authorizations	6.1, 8.1
NIST PE-3 Physical Access Control	6.2–6.5, 8.2–8.3
NIST PE-6 Monitoring Physical Access	6.5, 8.7
NIST PE-16 Delivery and Removal	6.8, 8.4



Morgan County System and Information Integrity Policy & Procedures

Document Number: MCIT-007

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. System and Information Integrity Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

This policy establishes requirements for protecting the integrity of Morgan County information systems by preventing, detecting, and responding to malware, unauthorized changes, vulnerabilities, and data integrity issues.

2. Authority

This policy supports the FBI Criminal Justice Information Services (CJIS) Security Policy v6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 System and Information Integrity (SI) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County-owned or managed servers, workstations, mobile devices, virtual machines, cloud services, applications, databases, network infrastructure, and security appliances.

4. Objectives

Maintain system integrity, reduce vulnerabilities, detect malicious activity, ensure timely remediation, protect data integrity, and provide auditable security processes.

5. Definitions

Key terms include Malware, Vulnerability, Integrity, Indicator of Compromise (IOC), Endpoint Detection and Response (EDR), Security Patch, and Unauthorized Change.

6. System and Information Integrity Policy

The following requirements establish the minimum system and information integrity controls for Morgan County information systems. These requirements apply to all production systems unless an approved exception exists.

6.1 Malware Protection

County-managed workstations and servers shall use centrally managed anti-malware and EDR technology configured for real-time protection, automatic security updates, and centralized alerting. Protection shall remain enabled unless temporarily disabled by authorized Information Technology personnel for approved maintenance or troubleshooting.

6.2 Endpoint Detection and Response (EDR)

EDR alerts shall be monitored and investigated. Confirmed malicious activity shall be handled in accordance with the Incident Response Plan (MCIT-008; Complete Policy, page 76).

6.3 Vulnerability Management

Security vulnerabilities shall be identified through vendor notifications, automated vulnerability assessments, threat intelligence, or other approved methods.

6.4 Security Patch Management

Security updates shall be evaluated and applied no later than the following maximum periods after release or identification: Critical within 15 calendar days, High within 30 calendar days, Medium within 60 calendar days, and Low within 90 calendar days. Information Technology may deploy updates sooner based on active exploitation, operational risk, or vendor guidance.

County-owned portable computers assigned for regular use shall be powered on and connected to the internet or County network at least once every seven calendar days for sufficient time to receive security updates and management instructions. Users shall complete required restarts promptly. Approved leave, emergency or continuity equipment, and other documented exceptions may follow an Information Technology-approved schedule.

6.5 Unauthorized Software

Unauthorized software shall not be installed on County systems. Information Technology may remove or disable unauthorized software without prior notice.

6.6 File & Data Integrity

Critical system files and sensitive data shall be protected against unauthorized modification. Integrity shall be verified following significant incidents or system recovery.

6.7 Threat Intelligence

Information Technology shall review relevant threat intelligence sources and evaluate significant threats affecting County technology.

6.8 Security Monitoring

Security monitoring shall include inbound and outbound communications at network boundaries; EDR, Security Information and Event Management (SIEM), firewall, gateway, cloud-service, and denial-of-service indicators; and other security alerts. Automated monitoring and alerting shall operate continuously, and designated Information Technology personnel shall review and investigate alerts as appropriate.

6.9 Indicators of Compromise

Known or suspected indicators of compromise shall be investigated promptly and escalated when appropriate.

6.10 Corrective Actions

Corrective actions shall be documented, tracked, and verified following significant integrity events.

6.11 Integrity Verification

System integrity shall be verified following malware removal, system restoration, or other significant recovery activities.

6.12 Security Testing

Security testing may be conducted following major system changes to verify continued integrity and security.

6.13 Annual Review

System and information integrity controls shall be reviewed at least annually and after significant technology changes.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight for the System and Information Integrity Program.
- Approve significant policy revisions and provide appropriate resources.

7.2 County Leadership

- Support implementation of system integrity controls.
- Ensure departments cooperate with remediation and incident response activities.

7.3 Information Technology Director

- Administer the System and Information Integrity Program.
- Approve integrity standards and significant corrective actions.
- Review security incidents affecting system integrity.
- Ensure annual integrity reviews are completed.

7.4 Department Heads

- Ensure personnel comply with integrity-related policies.

- Coordinate with IT when systems are affected by vulnerabilities or malware.
- Support timely remediation efforts.

7.5 System Owners

- Approve application-specific integrity requirements.
- Assist with vulnerability remediation and testing.
- Validate successful restoration of business applications after corrective actions.

7.6 Information Technology Staff

- Monitor EDR, SIEM, and security alerts.
- Deploy security patches in accordance with the Patch Management Policy.
- Investigate indicators of compromise.
- Perform malware remediation and integrity verification.
- Maintain documentation of corrective actions.

7.7 Supervisors

- Report suspected malware infections or system misuse.
- Ensure employees comply with security directives during incident response.

7.8 Users

- Do not disable approved security software.
- Promptly report suspicious emails, malware warnings, or unusual system behavior.
- Follow IT instructions during security incidents.

7.9 Contractors and Third Parties

- Comply with Morgan County system integrity requirements.
- Coordinate changes affecting County systems through Information Technology.
- Report suspected security events involving County resources immediately.

8. Operational Procedures

8.1 Vulnerability Identification and Assessment

1. Monitor vendor security advisories, threat intelligence, and vulnerability notifications.
2. Identify affected County systems and evaluate risk.

3. Prioritize remediation based on severity, exploitability, and business impact.
4. Document findings and remediation decisions.

8.2 Patch Evaluation and Deployment

1. Review available security updates and record the vendor severity or the County-assigned severity when the vendor does not provide one.
2. Test updates when practical, prioritizing rapid deployment when active exploitation or significant risk is present.
3. Deploy updates within the maximum deadlines of 15 days for Critical, 30 days for High, 60 days for Medium, and 90 days for Low severity; use emergency procedures when a normal maintenance window would miss the deadline.
4. Verify successful installation, document completion or failure, and remediate failed deployments within the applicable deadline.

8.3 Malware Response

1. Isolate affected systems when appropriate.
2. Investigate the scope of the infection using approved security tools.
3. Remove or quarantine malicious software.
4. Restore systems as needed and verify integrity before returning them to production.

8.4 Indicator of Compromise (IOC) Investigation

1. Review EDR, SIEM, firewall, and other security alerts.
2. Determine whether indicators represent confirmed or suspected compromise.
3. Escalate significant findings under the Incident Response Plan (MCIT-008; Complete Policy, page 77).
4. Document investigative actions and outcomes.

8.5 Security Monitoring

1. Review automated alerts from EDR, SIEM, firewalls, gateways, cloud services, and managed monitoring services.

2. Review inbound and outbound communications and denial-of-service indicators for unusual or unauthorized activity.
3. Escalate significant security events under the Incident Response Policy (MCIT-008; Complete Policy, page 77) and document the investigation and disposition.

8.6 Integrity Verification

1. Verify critical files, configurations, and applications following malware removal or system restoration.
2. Confirm normal system operation before returning services to production.

8.7 Unauthorized Software Response

1. Investigate unauthorized software installations.
2. Remove or disable unauthorized software when appropriate.
3. Document corrective actions.

8.8 Corrective Action Tracking

1. Track remediation activities until complete.
2. Verify corrective actions resolved the identified issue.
3. Retain supporting documentation.

8.9 Annual Integrity Review

1. Review malware protection effectiveness.
2. Review vulnerability management activities.
3. Review EDR and monitoring effectiveness.
4. Document recommendations and corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, vulnerability assessments, CJIS audits, and other authorized evaluations. Systems that do not meet integrity requirements shall be remediated based on risk.

- Approved anti-malware and EDR software shall remain enabled unless temporarily disabled by authorized IT personnel.
- Critical vulnerabilities shall be remediated in accordance with the Patch Management Policy.
- Unauthorized software may be removed from County-owned devices.
- Violations of this policy may result in disciplinary action or suspension of system access.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting Criminal Justice Information (CJI) or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

The following documentation should be retained to demonstrate implementation of this policy:

- Vulnerability assessment reports
- Patch deployment records
- Endpoint Detection and Response (EDR) alerts
- Malware investigation records
- Indicator of Compromise (IOC) investigations
- Security monitoring reports
- Integrity verification records
- Unauthorized software remediation records
- Corrective action documentation
- Annual integrity review reports

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 – System and Information Integrity (SI)
- National Institute of Standards and Technology (NIST) NIST SP 800-40 Guide to Enterprise Patch Management
- Morgan County Patch Management Policy
- Morgan County Incident Response Plan (MCIT-008; Complete Policy, page 74)
- Morgan County Configuration Management Policy (MCIT-010; Complete Policy, page 93)
- Morgan County Audit & Accountability Policy (MCIT-011; Complete Policy, page 104)

13. Revision History

Version	Date	Author	Description
1.0	07/01/2025	Jeremy Archibald	Patch Management v1.0; adopted 8/19/2025 (CR 25-45)
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; portable-device update connectivity and records disposition clarified; pending approval

Appendices, Forms & Checklists

Vulnerability Assessment Checklist

Complete	Task
☐	Vendor advisories reviewed
☐	Threat intelligence reviewed
☐	Affected assets identified
☐	Risk assigned
☐	Remediation scheduled

Patch Deployment Checklist

Complete	Task
☐	Patches evaluated
☐	Testing completed when practical
☐	Backups confirmed
☐	Patches deployed
☐	Installation verified
☐	Documentation updated

Malware Response Checklist

Complete	Task
☐	System isolated if required
☐	EDR investigation completed
☐	Malware removed or quarantined
☐	System restored
☐	Integrity verified

IOC Investigation Checklist

Complete	Task
☐	IOC validated
☐	Logs reviewed
☐	Scope determined
☐	Incident escalated if required
☐	Findings documented

Integrity Verification Checklist

Complete	Task
☐	Critical files verified
☐	Applications tested
☐	Security controls operational
☐	Services restored

Annual Integrity Review

Complete	Task
☐	EDR effectiveness reviewed
☐	Vulnerability process reviewed
☐	Patch compliance verified
☐	Corrective actions tracked
☐	Policy reviewed

Appendix – Recommended Records Retention

Maintain vulnerability reports, patch records, EDR alerts, malware investigations, integrity verification records, corrective actions, and annual reviews in accordance with CJIS requirements and County records retention schedules.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS System and Information Integrity	Sections 6–8
NIST SI-2 Flaw Remediation	6.3–6.4, 8.2
NIST SI-3 Malicious Code Protection	6.1–6.2, 8.3
NIST SI-4 System Monitoring	6.8–6.9, 8.4–8.5
NIST SI-7 Software, Firmware & Information Integrity	6.6, 6.11, 8.6



Morgan County Incident Response Policy & Procedures

Document Number: MCIT-008

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Overview
- 2. Purpose
- 2.1 Scope
- 3. Incident Response Goals
- 4. Definitions and Severity Levels
 - 4.1 Incident Definition
 - 4.2 Severity Levels
- 5. Roles and Responsibilities
- 6. Incident Response Procedures
 - 6.1 Preparation
 - 6.2 Discovery
 - 6.3 Notification
 - 6.4 Analysis and Assessment
 - 6.5 Response Strategy
 - 6.6 Containment
 - 6.7 Prevention of Re-Infection
 - 6.8 Restore Affected Systems
 - 6.9 Documentation
 - 6.10 Evidence Preservation
 - 6.11 External Notification
 - 6.12 Damage and Cost Assessment
 - 6.13 Post-Incident Review
- 7. Training, Testing, and Tabletop Exercises
- 8. Metrics and Reporting
- 9. Revision History
- Appendices

1. Overview

This plan defines what constitutes a security incident and outlines the structured phases of incident response. It designates roles, responsibilities, and steps for identification, containment, eradication, and recovery from cyber incidents.

2. Purpose

To ensure the protection of Morgan County's systems, networks, and data by complying with the FBI Criminal Justice Information Services (CJIS) Security Policy (Section 5.3), Utah Cyber Center guidance, and cybersecurity best practices.

2.1 Scope

This policy and its procedures apply to all Morgan County personnel, contractors, information systems, networks, cloud services, facilities, and information assets, including systems that process, store, or transmit Criminal Justice Information (CJI) or Personally Identifiable Information (PII).

3. Incident Response Goals

- Verify whether an incident occurred
- Maintain or restore service continuity
- Reduce impact and scope
- Determine the cause and methods
- Prevent recurrence
- Aid legal prosecution if applicable
- Keep county leadership informed

4. Definitions and Severity Levels

4.1 Incident Definition

An incident is defined as any event that threatens the confidentiality, integrity, or availability of County systems, including but not limited to: - Unauthorized access or modification - Malware infections - Theft or damage of hardware - Denial-of-service (DoS) attacks - Misuse of county resources - Unusual system behavior or Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) alerts

4.2 Severity Levels

Level	Description	Operational Response Target
S1 (Critical)	Major data breach,	1 hour

Level	Description	Operational Response Target
	widespread outage	
S2 (High)	Targeted malware, system compromise	4 hours
S3 (Medium)	Unauthorized access attempts	1 business day
S4 (Low)	Non-malicious anomalies	Logged only

5. Roles and Responsibilities

Incident Response Team (IRT)

- **Incident Commander (Information Technology Director)**
- Oversees incident response efforts
- Leads communication with leadership
- **IRT Coordinator**
- Manages workflows, escalations, and support tickets
- **IT Technical Lead**
- Leads containment, forensic analysis, and restoration
- **Communications Lead**
- Handles internal/external messaging and notifications
- **Legal and Compliance Liaison**
- Coordinates with County Attorney, Sheriff, and external agencies
- **Information Technology Staff and Technical Support**
- Assist in technical response and monitoring

6. Incident Response Procedures

6.1 Preparation

- Maintain current policies on passwords, intrusion detection, backups, and contact procedures
- Maintain up-to-date firewall, antivirus, and endpoint protection
- Conduct annual tabletop exercises

6.2 Discovery

- Incidents may be detected by:
- Information Technology Director, Information Technology Staff, County Employees, Monitoring Systems

6.3 Notification

Personnel shall report suspected security incidents to the Information Technology Department or County Incident Response Team (IRT) immediately and no later than one (1) hour after discovery. The Incident Commander shall record the discovery and reporting times and activate the emergency contact tree for the County Commission Chair, UCIP Cybersecurity Insurance, Utah Cyber Center/SLCGP, and the Sheriff and County Attorney as needed.

6.4 Analysis and Assessment

Evaluate: - Whether the incident is real or perceived - Threat level and criticality of affected systems - Potential impact to business operations - Scope: local vs. network-wide

6.5 Response Strategy

- Evaluate urgency and risk of tipping off attacker
- Determine whether rapid containment is possible

6.6 Containment

- Disconnect affected systems
- Change passwords
- Block suspicious IPs or ports

6.7 Prevention of Re-Infection

- Determine vector (email, ports, unpatched systems)
- Patch systems and close unnecessary ports/services
- Adjust email security settings
- Provide user retraining
- Disable unneeded services

6.8 Restore Affected Systems

- Reimage compromised systems as needed
- Restore from verified clean backups
- Enforce password changes
- Enable proper logging and monitoring

6.9 Documentation

- Log all incidents via support tickets

- Include: how, where, response steps, outcome, and effectiveness

6.10 Evidence Preservation

- Secure logs, screenshots, system images, emails
- Fill out Chain of Custody forms for legal evidence

6.11 External Notification

- Notify required entities:
- County Commission Chair
- UCIP
- Utah Cyber Center / SLCGP
- County Attorney and Sheriff if prosecution is likely
- Report every suspected or actual security breach involving CJI to the Utah CJIS ISO as soon as possible through the current Utah DPS CJIS incident-reporting channel. Current contact: Tyson Jarrett, tjarrett@utah.gov, 385-255-0888. Verify the contact information during the annual policy review and before each tabletop exercise.
- Notify affected product or service providers and other supply-chain parties when the incident involves their systems, products, or services.

6.12 Damage and Cost Assessment

- Estimate downtime costs, service disruptions, staff hours, and damage

6.13 Post-Incident Review

- Analyze lessons learned
- Identify broken procedures
- Update policies and tools to prevent recurrence
- Submit full incident report to County Leadership

7. Training, Testing, and Tabletop Exercises

- All IRT members must complete annual incident response training
- County will conduct at least one tabletop exercise per year
- Findings from drills will inform plan updates

8. Metrics and Reporting

Each incident response concludes with a report including: - Timeline of events - Systems affected
- Root cause and scope - Actions taken and effectiveness - Recommendations

Quarterly reports will be delivered to County Leadership summarizing incidents, trends, and response metrics.

9. Revision History

Version	Date	Author	Description
1.0	09/15/2023	Information Technology Director	Initial release
1.2	09/17/2024	Information Technology Director / CPO	Added severity levels, IRT roles, chain of custody, drills, and metrics
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

Incident Response Checklist

Complete	Task
☐	Suspected incident reported within one hour
☐	Severity classified
☐	Stakeholders notified
☐	Containment completed
☐	Evidence preserved
☐	Eradication completed
☐	Recovery validated
☐	Incident closed
☐	Confirmed CJI incident reported to the appropriate CJIS official

Evidence Collection Checklist

Complete	Task
☐	Relevant logs collected
☐	System images captured if required
☐	Chain of custody initiated
☐	Evidence securely stored

Post-Incident Review Checklist

Complete	Task
☐	Lessons learned meeting held
☐	Root cause identified
☐	Corrective actions assigned
☐	Documentation completed

Annual Incident Response Review

Complete	Task
☐	Incident Response Plan reviewed
☐	Exercise conducted
☐	Contact list verified
☐	Training completed
☐	Improvements documented

Appendix – Recommended Records Retention

Retain incident reports, evidence records, chain of custody documentation, exercise records, lessons learned reports, and corrective action records in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or National Institute of Standards and Technology (NIST) guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Incident Response	Sections 6–8
NIST IR-4 Incident Handling	6.2–6.10, 8.1–8.6
NIST IR-5 Incident Monitoring	6.2, 8.1–8.2
NIST IR-6 Incident Reporting, including IR-6(1)	6.3, 6.9, 6.11

Control	Policy Section
and IR-6(3)	
NIST IR-8 Incident Response Plan	6.1, 6.12–6.13



Morgan County Identification & Authentication Policy & Procedures

Document Number: MCIT-009

Version: 1.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Identification & Authentication Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

This policy establishes requirements for uniquely identifying users, authenticating access to Morgan County information systems, protecting authentication credentials, and supporting accountability for all access to County resources.

2. Authority

This policy supports the FBI Criminal Justice Information Services (CJIS) Security Policy v6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Identification and Authentication (IA) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County-owned or managed systems, cloud services, applications, network devices, remote access solutions, privileged accounts, service accounts, and users accessing County information resources.

4. Objectives

Ensure each user has a unique identity, require strong authentication, protect credentials, require multi-factor authentication (MFA) on all County-owned computers for privileged and non-privileged accounts, and provide auditable authentication events.

5. Definitions

Key terms include Authentication, MFA, Service Account, Privileged Account, Shared Account, Credential, and Identity Provider.

6. Identification & Authentication Policy

The following requirements establish the minimum identification and authentication controls for Morgan County information systems. These requirements apply to all production systems unless an approved exception exists.

6.1 Unique User Identification

Each individual shall be assigned a unique user identifier. Shared user accounts are prohibited except where specifically approved, documented, and technically unavoidable.

6.2 Authentication

Users shall authenticate using approved methods before accessing County systems, applications, or networks.

6.3 Password Requirements

Passwords shall comply with current Morgan County standards and applicable CJIS requirements. Default vendor passwords shall be changed before systems are placed into production.

6.4 Multi-Factor Authentication (MFA)

MFA shall be required on all County-owned computers and for access to privileged and non-privileged accounts, including local, network, and remote access. Approved methods are an

authenticator application using push approval or a time-based one-time password (TOTP), or an approved hardware token or security key. Email-delivered PINs or one-time passcodes shall not be used for County-controlled authentication systems. They may be used when required by an externally managed government service for which the County cannot select another authentication method, including the State of Utah UtahID system used to access the CJIS audit site. This exception is limited to that external service and does not authorize email-delivered codes for County-controlled systems. SMS is a restricted transitional method and may be used only with a documented migration plan to an approved authenticator application or hardware token. MFA shall be implemented for all Criminal Justice Information (CJI) systems in accordance with CJIS IA-2(1) and IA-2(2).

6.5 Privileged Accounts

Administrative accounts shall be issued only to authorized personnel with a documented business need and shall be reviewed periodically.

6.6 Service Accounts

Service accounts shall be uniquely identified, documented, limited to their intended purpose, and protected with appropriately managed credentials.

6.7 Shared Accounts

If a shared account is exceptionally required, its use shall be approved, documented, monitored, and reviewed on a regular basis.

6.8 Credential Protection

Users shall not share passwords, PINs, MFA factors, screen-unlock credentials, or other authentication credentials. Credentials shall not be stored in plain text or transmitted in an unsecured manner. Information Technology shall use approved administrative recovery mechanisms or device-recovery keys to recover, reset, lock, or wipe County-owned equipment without obtaining or retaining a user's authentication credential.

6.9 Password Reset

Identity shall be verified before resetting passwords or issuing temporary credentials.

6.10 Account Lockout

Systems shall implement account lockout or equivalent protections against repeated failed authentication attempts where technically feasible.

6.11 Authentication Logging

Authentication successes, failures, lockouts, and privileged authentication events shall be logged in accordance with the Audit & Accountability Policy (MCIT-011; Complete Policy, page 105).

6.12 Remote Access

Remote access shall use approved authentication methods and comply with County remote access requirements.

6.13 Credential Review

Privileged accounts, service accounts, and authentication mechanisms shall be reviewed periodically for continued business need and security.

6.14 Annual Review

Identification and authentication controls shall be reviewed at least annually and after significant technology changes.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight for the Identification & Authentication Program.
- Approve significant policy revisions and support necessary resources.

7.2 County Leadership

- Promote compliance with authentication requirements.
- Support corrective actions when deficiencies are identified.

7.3 Information Technology Director

- Administer the Identification & Authentication Program.
- Approve authentication standards and privileged access.
- Ensure MFA is implemented and verified on all County-owned computers and for all privileged and non-privileged accounts.
- Review the program annually.

7.4 Department Heads

- Approve access requests based on business need.
- Promptly notify IT of staffing changes affecting accounts.
- Verify users retain a legitimate business need for access.

7.5 System Owners

- Approve application-specific authentication requirements.
- Review privileged and service account usage.
- Participate in periodic account reviews.

7.6 Information Technology Staff

- Create, modify, disable, and remove user accounts.
- Implement MFA and password standards.
- Verify identity before password resets.
- Maintain authentication logs and account records.

7.7 Supervisors

- Ensure employees follow authentication requirements.
- Report suspected credential compromise immediately.

7.8 Users

- Protect authentication credentials.
- Never share passwords or MFA tokens.
- Report lost devices or suspected account compromise immediately.

7.9 Contractors and Third Parties

- Use only authorized accounts.
- Comply with County authentication requirements and return authentication devices upon contract completion.

8. Operational Procedures

8.1 New Account Provisioning

1. Department Head submits an approved access request.

2. IT verifies the user's identity and business need.
3. Create a unique user account using least privilege.
4. Configure and verify MFA for every County-owned computer and for all privileged and non-privileged user accounts.
5. Document account creation and notify the requester.

8.2 Account Modification

1. Review requested changes for business justification.
2. Remove unnecessary access before granting additional privileges.
3. Document all significant account modifications.

8.3 Password Reset

1. Verify the user's identity using approved methods.
2. Issue a temporary password or reset link.
3. Require the user to change the password at first sign-in where supported.
4. Document the reset if required.

8.4 MFA Enrollment and Recovery

1. Verify the user's identity, enroll the user in an approved authenticator application or hardware factor, and document the assigned factor type.
2. Test the factor on applicable County-owned computers and CJI systems before access is considered complete.
3. Provide recovery or re-enrollment only after identity verification; promptly replace or revoke lost or compromised authentication devices.

8.5 Privileged Account Administration

1. Maintain separate administrative accounts whenever practical.
2. Review privileged accounts periodically.
3. Remove elevated privileges when no longer required.

8.6 Service Account Management

1. Document the purpose and owner of each service account.
2. Limit permissions to the minimum necessary.
3. Review service account credentials periodically.

8.7 Account Disablement

1. Disable accounts promptly following termination or direction from authorized management.
2. Revoke VPN, MFA, and other remote access methods.
3. Document completion of the offboarding process.

8.8 Authentication Logging

1. Record successful and failed authentication events where supported.
2. Forward logs to centralized logging systems when available.
3. Investigate repeated authentication failures.

8.9 Annual Review

1. Review authentication settings, privileged accounts, MFA deployment, and service accounts.
2. Document findings and corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, and CJIS or other authorized audits. Authentication controls shall be evaluated to ensure they remain effective and appropriate.

- Unique user accounts shall be used where required.
- MFA shall be enforced on all County-owned computers and for privileged and non-privileged accounts.
- Authentication records shall be protected and retained in accordance with applicable requirements.
- Violations of this policy may result in disciplinary action or suspension of system access.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

The following documentation should be retained to demonstrate implementation of this policy:

- Account request and approval records
- Account provisioning records
- Password reset documentation
- MFA enrollment records
- Privileged account review reports
- Service account inventory and review records
- Authentication log reports
- Account disablement records
- Annual authentication review documentation
- Corrective action records

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 – Identification & Authentication (IA)
- National Institute of Standards and Technology (NIST) NIST SP 800-63 Digital Identity Guidelines
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)
- Morgan County Audit & Accountability Policy (MCIT-011; Complete Policy, page 104)
- Morgan County Personnel Security Policy (MCIT-002; Complete Policy, page 11)

13. Revision History

Version	Date	Author	Description
1.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; credential protection, administrative recovery, and records disposition clarified; pending approval

Appendices, Forms & Checklists

New Account Request

Complete	Task
☐	Business needs documented
☐	Department Head approval received
☐	Identity verified
☐	Least privilege applied
☐	MFA configured and verified
☐	User notified

Password Reset

Complete	Task
☐	Identity verified
☐	Temporary credential issued
☐	User required to change password
☐	Reset documented if required

MFA Enrollment

Complete	Task
☐	Approved MFA method enrolled
☐	Recovery information verified
☐	User tested authentication
☐	Enrollment documented

Privileged Account Review

Complete	Task
☐	Business need verified
☐	Administrative access validated

Complete	Task
☐	Inactive privileged accounts removed
☐	Review documented

Service Account Review

Complete	Task
☐	Owner identified
☐	Purpose documented
☐	Credentials reviewed
☐	Permissions validated

Account Termination

Complete	Task
☐	Account disabled
☐	VPN access revoked
☐	MFA revoked
☐	Privileged access removed
☐	Completion documented

Annual Authentication Review

Complete	Task
☐	Authentication standards reviewed
☐	MFA coverage verified
☐	Service accounts reviewed
☐	Privileged accounts reviewed
☐	Corrective actions documented

Appendix – Recommended Records Retention

Maintain account requests, approvals, authentication logs, password reset documentation, MFA enrollment records, privileged account reviews, service account documentation, and annual reviews in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Identification & Authentication	Sections 6–8
NIST IA-2(1) / IA-2(2) MFA for Privileged and Non-Privileged Accounts	6.1–6.4, 8.1, 8.4



Morgan County Configuration Management Policy & Procedures

Document Number: MCIT-010

Version: 1.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Configuration Management Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

This policy establishes requirements for managing and controlling changes to Morgan County information systems to ensure confidentiality, integrity, availability, and compliance with CJIS. It defines how systems are baselined, documented, approved, modified, and monitored throughout their lifecycle.

2. Authority

This policy is established under the authority of the Morgan County Commission and supports the FBI Criminal Justice Information Services (CJIS) Security Policy v6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Configuration Management controls, Utah law, and Morgan County information security policies.

3. Scope

Applies to all County-owned or managed servers, workstations, laptops, network devices, firewalls, virtual infrastructure, cloud services, applications, databases, and security appliances used to process, store, or transmit County information.

4. Objectives

Maintain secure baseline configurations, document and approve changes, reduce operational risk, support rapid recovery, maintain accurate inventories, and provide auditable evidence of configuration management activities.

5. Definitions

Configuration Item (CI), Baseline Configuration, Change Request, Emergency Change, Rollback Plan, Configuration Drift, and System Owner are key terms used throughout this policy.

6. Configuration Management Policy

The following requirements establish the minimum configuration management controls for Morgan County information systems. These requirements apply to all production systems unless an approved exception exists.

6.1 Baseline Configurations

Secure baseline configurations shall be established, documented, approved, and maintained for servers, workstations, network devices, firewalls, virtual infrastructure, cloud services, and security appliances. Baseline documentation shall include a current topological network diagram showing devices, physical and logical links, network boundaries, external connections, and the flow of Criminal Justice Information (CJI) and other sensitive data.

6.2 Configuration Identification

Configuration Items (CIs) shall be uniquely identified and tracked throughout their lifecycle.

6.3 Hardware Inventory

Information Technology shall maintain an accurate inventory of County-owned computing and network equipment. Records shall include, as applicable, component type, physical or logical location, manufacturer, model, serial or asset number, installation or acquisition date, supplier, owner or custodian, and lifecycle status.

6.4 Software Inventory

Information Technology shall maintain the Morgan County Approved Applications and Software Register as the authoritative operational list of software, cloud services, and applications approved for County use. The register shall document approved use and scope, restrictions, ownership, approval basis, review dates, and supporting evidence; it shall be reviewed at least annually and updated when an item is approved, materially changed, restricted, suspended, retired, or prohibited. Automated software inventory and endpoint-management records shall be reconciled against the register. Unauthorized software may be removed or disabled.

6.5 Change Requests

Production configuration changes shall be documented and approved before implementation except during emergencies.

6.6 Standard Changes

Routine, low-risk changes may follow an approved standard change process.

6.7 Emergency Changes

Emergency changes may be implemented to restore service or mitigate risk but shall be documented and reviewed after implementation.

6.8 Rollback Planning

Changes that could affect production services shall include a documented rollback or recovery plan.

6.9 Secure Configuration Standards

Default passwords shall be changed, unnecessary services disabled, and vendor security recommendations followed where practical.

County-managed systems shall use approved administrative recovery mechanisms or centrally controlled device-recovery keys where supported. Recovery material shall be restricted to authorized Information Technology personnel, protected from unauthorized disclosure, and maintained so County-owned equipment can be recovered, reset, locked, or wiped without obtaining or retaining a user's authentication credential.

6.10 Configuration Drift

Periodic reviews shall identify unauthorized or unintended configuration changes.

6.11 Network Devices

Router, switch, wireless, firewall, and VPN configurations shall be backed up and protected from unauthorized modification.

6.12 Virtual Infrastructure

Hypervisors and virtual machines shall follow documented configuration standards and be included in change management.

6.13 Cloud Services

Configuration changes affecting cloud-hosted systems shall follow the same approval process as on-premises systems.

6.14 Configuration Monitoring

Critical configuration changes shall be monitored and investigated when unauthorized activity is suspected.

6.15 Documentation

Configuration documentation shall identify the requester, approver, implementer, implementation date, affected systems, and completion status.

6.16 Annual Review

Baseline configurations shall be reviewed at least annually and after major technology changes.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight for the County Configuration Management Program.
- Approve significant policy changes and allocate appropriate resources.

7.2 County Leadership

- Support compliance with configuration management requirements.
- Ensure departments follow approved change processes.

7.3 Information Technology Director

- Administer the Configuration Management Program.
- Approve significant or high-risk production changes.
- Review emergency changes after implementation.
- Ensure annual baseline reviews are completed.

7.4 Department Heads

- Approve configuration changes affecting departmental operations.
- Coordinate maintenance windows with Information Technology.
- Participate in post-change validation when appropriate.

7.5 System Owners

- Approve application-specific changes.
- Validate successful implementation.
- Identify business impacts and rollback requirements.

7.6 Information Technology Staff

- Maintain baseline configurations.
- Implement approved changes.
- Document configuration changes.
- Maintain configuration backups and inventories.

7.7 Change Requestors

- Submit complete change requests with business justification.
- Identify affected systems and expected impact.
- Provide rollback information when applicable.

7.8 Change Approvers

- Review technical, operational, and security impacts.
- Approve, reject, or request modification of proposed changes.
- Ensure emergency changes receive post-implementation review.

7.9 Vendors and Contractors

- Follow Morgan County configuration standards.
- Obtain approval before implementing production changes.
- Document all work performed on County systems.

8. Operational Procedures

8.1 Standard Change Process

1. Submit a documented Change Request identifying the business need, affected systems, implementation window, and rollback plan.
2. Obtain approval from the appropriate Department Head, System Owner, and Information Technology.
3. Notify affected users when service interruptions are expected.
4. Back up affected configurations before implementation whenever practical.
5. Implement the approved change during the authorized maintenance window.
6. Validate successful operation and document the results.

8.2 Emergency Change Process

1. Emergency changes may be implemented to restore critical services or address significant security risks.
2. Notify the Information Technology Director as soon as practical.
3. Document the reason for the emergency change.
4. Review the change after implementation and update documentation.

8.3 Baseline Configuration Management

1. Maintain approved baseline configurations for servers, workstations, network devices, virtualization platforms, cloud services, and security appliances.
2. Review baselines and the topological network diagram at least annually and after major infrastructure, connection, or CJI data-flow changes.

8.4 Configuration Backups

1. Back up firewall, switch, router, wireless controller, virtualization host, and other critical configurations before significant changes whenever practical.
2. Store configuration backups in a secure location with restricted access.

8.5 Rollback Procedures

1. Each significant production change shall include a documented rollback plan.
2. Rollback procedures shall be tested when practical for high-risk changes.

8.6 Inventory Maintenance

1. Update the hardware inventory and Approved Applications and Software Register whenever equipment, software, or a service is approved, added, removed, reassigned, materially modified, restricted, or retired.
2. Reconcile the register and inventories with automated software-inventory, endpoint-management, physical, and administrative records at least annually; record the review in the register Change Log and retain the evidence for audit purposes.

8.7 Cloud and Virtual Infrastructure

1. Apply the same approval and documentation requirements to cloud-hosted systems and virtual infrastructure.
2. Document changes to virtual networking, storage, templates, and security settings.

8.8 Documentation Requirements

Record the requester, approver, implementer, implementation date, systems affected, validation results, and completion status for significant changes.

8.9 Annual Configuration Review

1. Review baseline configurations.
2. Review privileged configuration changes.
3. Verify inventory accuracy.
4. Document findings and corrective actions.

9. Compliance

Morgan County shall periodically review compliance with this policy through internal reviews, management oversight, configuration audits, and external assessments. Unauthorized configuration changes or failure to follow approved change management procedures may result in disciplinary action.

- Production systems may be audited for configuration compliance.
- Configuration documentation shall be retained for audit purposes.
- Unauthorized software or configuration changes may be removed or reversed.
- Exceptions shall be documented and approved.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

The following records should be retained as evidence that this policy is implemented:

- Approved Change Requests
- Emergency Change documentation
- Configuration baseline documents
- Firewall, switch, and router configuration backups
- Virtual infrastructure configuration records
- Cloud configuration change records
- Hardware inventory reports
- Approved Applications and Software Register, Change Log, and software-inventory reports
- Annual baseline review documentation
- Rollback documentation
- Configuration audit reports

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 – Configuration Management (CM)

- National Institute of Standards and Technology (NIST) NIST SP 800-128 Guide for Security-Focused Configuration Management
- Morgan County Patch Management Policy (implemented through MCIT-007; Complete Policy, page 63)
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)
- Morgan County Audit & Accountability Policy (MCIT-011; Complete Policy, page 104)
- Morgan County Incident Response Plan (MCIT-008; Complete Policy, page 74)
- Morgan County System & Information Integrity Policy (MCIT-007; Complete Policy, page 63)

13. Revision History

Version	Date	Author	Description
1.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; managed device-recovery and records-disposition controls added; pending approval

Appendices, Forms & Checklists

Appendix A – Configuration Change Request

Each production configuration change should document the requester, business justification, affected systems, implementation window, risk assessment, rollback plan, approvals, and validation results.

Standard Change Checklist

Complete	Task
☐	Business justification documented
☐	Risk assessed
☐	Approvals obtained
☐	Users notified if required
☐	Configuration backup completed
☐	Rollback plan documented
☐	Change implemented
☐	Validation completed
☐	Documentation updated

Emergency Change Checklist

Complete	Task
☐	Emergency confirmed
☐	Information Technology Director notified
☐	Temporary mitigation documented
☐	Change implemented
☐	Post-implementation review completed
☐	Documentation finalized

Configuration Backup Checklist

Complete	Task
☐	Firewall configuration backed up
☐	Switch configuration backed up
☐	Router configuration backed up
☐	Virtual infrastructure exported
☐	Backup stored securely
☐	Restore verified when practical

Annual Baseline Review

Complete	Task
☐	Server baselines reviewed
☐	Workstation baselines reviewed
☐	Network device baselines reviewed
☐	Cloud configuration reviewed
☐	Security appliance configuration reviewed
☐	Corrective actions documented

Hardware Inventory Verification

Complete	Task
☐	Inventory current
☐	Retired assets removed
☐	New assets recorded
☐	Serial numbers verified
☐	Ownership confirmed

Software Inventory Verification

Complete	Task
☐	Approved Applications and Software Register updated
☐	Approved software and services reviewed

Complete	Task
☐	Unauthorized or unlisted software identified
☐	Ownership, licensing, conditions, evidence, and review dates verified

Appendix B – Recommended Records Retention

Maintain change requests, approval records, inventories, baseline documentation, configuration backups, annual reviews, and configuration audit reports in accordance with County retention schedules and applicable legal requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix C – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix D – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Configuration Management	Sections 6–8
NIST CM-2 Baseline Configuration	6.1–6.2, 6.9–6.10, 8.3
NIST CM-3 Configuration Change Control	6.5–6.8, 8.1–8.2
NIST CM-5 Access Restrictions for Change	6.5–6.7, 7.3–7.9, 8.1–8.2
NIST CM-6 Configuration Settings	6.9–6.14, 8.3–8.4, 8.7
NIST CM-8 System Component Inventory	6.3–6.4, 8.6

Morgan County Audit & Accountability Policy & Procedures

Document Number: MCIT-011

Version: 1.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Audit & Accountability Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

This policy establishes requirements for generating, protecting, reviewing, retaining, and using audit records to support accountability, security monitoring, incident investigations, and compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy and other applicable requirements.

2. Authority

This policy is established under the authority of the Morgan County Commission and supports the FBI CJIS Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Audit and Accountability (AU) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

This policy applies to all County-owned or managed servers, workstations, network devices, firewalls, virtual infrastructure, cloud services, applications, databases, and security appliances that process, store, or transmit County information.

4. Objectives

Maintain reliable audit logs, ensure accurate event attribution, support investigations, protect audit records from unauthorized modification, meet retention requirements, and provide verifiable evidence during audits.

5. Definitions

Key terms include Audit Record, Audit Log, Security Event, Time Synchronization, Chain of Custody, Security Information and Event Management (SIEM), and Privileged Activity.

6. Audit & Accountability Policy

The following requirements establish the minimum audit and accountability controls for Morgan County information systems. These requirements apply to all production systems unless an approved exception exists.

6.1 Audit Log Generation and Content

Systems shall generate sufficient audit records to reconstruct security-relevant events and support investigations. Each audit record shall contain, at minimum, the event type, date and time, outcome (success or failure), and the identity of the user, service account, or process associated with the event. Source device, destination, and other event details shall be recorded when supported by the system.

6.2 Auditable Events

At a minimum, successful and failed logons, account management, privilege changes, policy changes, configuration changes, system startup/shutdown, malware detections, and security alerts shall be logged.

6.3 User Attribution

Audit records shall uniquely identify the user, service account, or process responsible for each recorded event whenever technically feasible.

6.4 Log Protection

Audit logs shall be protected against unauthorized access, modification, deletion, and disclosure.

6.5 Log Integrity

Mechanisms shall be used where practical to detect unauthorized modification of audit records.

6.6 Log Retention

Audit records shall be retained for a minimum of one (1) year and longer when needed for administrative, legal, audit, investigative, or other operational purposes, in accordance with CJIS, Utah, and County requirements.

6.7 Time Synchronization

Systems generating audit logs shall synchronize to approved time sources to ensure accurate event correlation.

6.8 Routine Log Review

Audit records for systems that process, store, or transmit Criminal Justice Information (CJI) shall be reviewed and analyzed at least weekly. Other security logs shall be reviewed on a documented, risk-based schedule, with priority given to critical infrastructure. Continuous automated monitoring and alerting supplements but does not replace the documented weekly CJI audit-record review.

6.9 Privileged Activity

Administrative and privileged account activity shall receive additional monitoring and review.

6.10 SIEM Integration

Where available, centralized logging or SIEM solutions shall collect and correlate security events from critical systems.

6.11 Incident Evidence

Audit records relevant to suspected security incidents shall be preserved as evidence.

6.12 Chain of Custody

Evidence collected for investigations shall be documented to preserve integrity and admissibility where applicable.

6.13 Administrative Monitoring

Changes affecting security controls or system configurations shall be auditable.

6.14 Reporting

Significant security events shall be reported to appropriate management in accordance with the Incident Response Plan (MCIT-008; Complete Policy, page 77).

6.15 Annual Review

Audit logging configurations and review procedures shall be evaluated at least annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight for the County Audit & Accountability Program.
- Approve significant policy revisions and provide resources for implementation.

7.2 County Leadership

- Promote compliance with audit and accountability requirements.
- Support corrective actions identified through audits or investigations.

7.3 Information Technology Director

- Administer the Audit & Accountability Program.
- Ensure audit logging is enabled on critical systems.
- Review significant audit findings and coordinate corrective actions.
- Ensure annual reviews of logging and monitoring controls are completed.

7.4 Department Heads

- Ensure personnel comply with this policy.
- Review reports affecting their departments and assist with investigations.

7.5 System Owners

- Approve application-specific logging where appropriate.
- Validate logging requirements for business applications.
- Support log reviews and incident investigations.

7.6 Information Technology Staff

- Configure and maintain audit logging.
- Protect audit records from unauthorized modification.
- Review security events and escalate suspicious activity.
- Document weekly CJI audit-record reviews and provide significant findings to the Information Technology Director and, when applicable, the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO).
- Maintain time synchronization and log retention settings.

7.7 Supervisors

- Report suspected policy violations or misuse.
- Cooperate with investigations involving personnel under their supervision.

7.8 Users

- Use County systems only for authorized purposes.
- Immediately report suspected security incidents or unauthorized activity.

7.9 Contractors and Third Parties

- Comply with County logging and audit requirements applicable to services they provide.
- Cooperate with authorized investigations and preserve relevant records when requested.

8. Operational Procedures

8.1 Routine and Weekly CJI Log Review

1. Review critical dashboards, monitoring systems, and alerts according to the operating schedule.
2. At least weekly, review and analyze audit records for systems that process, store, or transmit CJI.

3. Review failed authentication attempts and privileged activity during the applicable review.
4. Investigate unusual or suspicious events.
5. Document the date, reviewer, log sources, significant findings, and corrective actions.
6. Escalate significant findings to the Information Technology Director and, for CJI matters when applicable, the TAC and LASO.

8.2 Security Event Escalation

1. Classify the event based on severity and potential impact.
2. Notify the Information Technology Director for significant events.
3. Initiate the Incident Response Plan (MCIT-008; Complete Policy, page 76) when appropriate.

8.3 Incident Evidence Preservation

1. Preserve relevant audit logs before making system changes.
2. Export logs in a manner that maintains integrity.
3. Capture supporting evidence such as screenshots when appropriate.
4. Document all actions taken.

8.4 Chain of Custody

1. Document who collected evidence.
2. Record the date and time of collection.
3. Maintain custody records whenever evidence may support administrative, civil, or criminal proceedings.

8.5 Time Synchronization

1. Verify that systems synchronize with approved time sources.
2. Investigate and correct significant time drift.

8.6 Log Retention

1. Retain audit logs for a minimum of one (1) year and longer when required for administrative, legal, audit, investigative, or operational purposes.
2. Protect archived logs from unauthorized modification or deletion.

8.7 SIEM / Centralized Logging

1. Forward logs from critical systems to centralized logging where available.
2. Review correlated alerts generated by the monitoring platform.

8.8 Administrative Activity Review

1. Review privileged account activity periodically.
2. Investigate unauthorized administrative actions.

8.9 Annual Audit Program Review

1. Review logging configuration on critical systems.
2. Verify log retention settings.
3. Evaluate monitoring effectiveness.
4. Document recommendations and corrective actions.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, CJIS audits, and other authorized assessments. Audit and accountability controls shall be tested to ensure they remain effective and appropriate.

- Critical systems shall maintain required audit logging.
- Audit logs shall be protected from unauthorized access or modification.
- Log review activities shall be documented.
- Failure to comply with this policy may result in disciplinary action, suspension of access, or other corrective measures.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and

compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the TAC and LASO and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

The following documentation should be retained to demonstrate implementation of this policy:

- Documented routine and at-least-weekly CJI audit-record review records
- SIEM alert reports
- Incident investigation logs
- Chain of custody documentation
- Time synchronization verification records
- Administrative activity review reports
- Audit configuration documentation
- Audit log retention records
- Security event reports
- Corrective action documentation
- Annual audit program review records
- Representative audit-log export or screenshots showing event type, date and time, outcome, and user, service-account, or process attribution

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0 — AU-6 Audit Record Review, Analysis, and Reporting
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 — AU-6 Audit Record Review, Analysis, and Reporting
- National Institute of Standards and Technology (NIST) NIST SP 800-92 Guide to Computer Security Log Management
- Morgan County Incident Response Plan (MCIT-008; Complete Policy, page 74)
- Morgan County Access Control Policy (MCIT-003; Complete Policy, page 24)
- Morgan County Configuration Management Policy (MCIT-010; Complete Policy, page 93)
- Morgan County System & Information Integrity Policy (MCIT-007; Complete Policy, page 63)

13. Revision History

Version	Date	Author	Description
1.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

Appendix A – Routine and Weekly CJI Log Review

Routine and Weekly CJI Log Review

Complete	Task
☐	CJI-system audit records reviewed at least weekly
☐	Other critical systems reviewed according to schedule
☐	Failed authentication attempts reviewed
☐	Privileged account activity reviewed
☐	Security alerts investigated
☐	Findings documented
☐	Review date, reviewer, and log sources documented

SIEM / Centralized Logging Review

Complete	Task
☐	SIEM operational
☐	Critical log sources reporting
☐	High-severity alerts reviewed
☐	False positives documented
☐	Escalations completed

Incident Evidence Collection

Complete	Task
☐	Relevant logs preserved
☐	Screenshots collected if appropriate
☐	Evidence exported
☐	Integrity maintained
☐	Incident record updated

Appendix B – Chain of Custody Form

Document the evidence description, source system, date/time collected, collector, transfer history, storage location, and final disposition for evidence retained during investigations.

Time Synchronization Verification

Complete	Task
☐	Approved time source configured
☐	Time synchronization verified
☐	Significant drift corrected
☐	Verification documented

Log Retention Review

Complete	Task
☐	One-year minimum retention verified
☐	Archived logs protected
☐	Expired logs handled per retention schedule
☐	Review documented

Annual Audit Program Review

Complete	Task
☐	Logging configuration reviewed
☐	Log review procedures evaluated
☐	SIEM configuration reviewed
☐	Corrective actions documented
☐	Policy review completed

Appendix C – Recommended Records Retention

Retain audit logs for a minimum of one (1) year and retain review records, investigation documentation, chain of custody records, time synchronization verification, SIEM reports, and annual audit reviews in accordance with CJIS requirements, Utah records retention schedules, and County policy.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix D – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix E – CJIS & NIST Control Mapping

Control	Policy Section
FBI CJIS v6.0 AU-6 Audit Record Review, Analysis, and Reporting	6.8, 8.1
NIST AU-2 Audit Events	6.2
NIST AU-3 Content of Audit Records	6.1–6.3
NIST AU-6 Audit Review	6.8, 8.1
NIST AU-8 Time Stamps	6.7, 8.5
NIST AU-9 Protection of Audit Information	6.4–6.6
NIST AU-11 Audit Record Retention	6.6, 8.6



Morgan County Risk Assessment Policy & Procedures

Document Number: MCIT-012

Version: 1.1 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Risk Assessment Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements for identifying, evaluating, documenting, prioritizing, and managing risks to Morgan County information systems, information assets, and Criminal Justice Information (CJI).

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Risk Assessment (RA) and Assessment, Authorization, and Monitoring (CA) controls, applicable Utah law, and Morgan County information security policies.

3. Scope

Applies to all County departments, information systems, cloud services, applications, infrastructure, third-party services, and business processes supporting County operations.

4. Objectives

Provide a consistent methodology for identifying and evaluating risk, supporting informed risk decisions, and reducing cybersecurity risk through appropriate mitigation strategies.

5. Definitions

Key terms include Risk, Threat, Vulnerability, Likelihood, Impact, Risk Owner, Residual Risk, Risk Acceptance, Formal Risk Assessment, and Production Authorization.

6. Risk Assessment Policy

The following requirements establish the minimum risk assessment requirements for Morgan County information systems and information assets.

6.1 Risk Assessment Program

Morgan County shall maintain a documented risk assessment program.

6.2 Asset Identification

Information assets shall be identified and evaluated based on business importance.

6.3 Threat Identification

Relevant internal and external threats shall be identified.

6.4 Vulnerability Assessment

Known vulnerabilities shall be identified through assessments, vendor notifications, and security monitoring.

6.5 Risk Analysis

Risks shall be evaluated based on likelihood and potential impact.

6.6 Risk Prioritization

Risks shall be prioritized to support mitigation planning.

6.7 Risk Treatment

Risks shall be mitigated, transferred, accepted, or avoided based on management decisions.

6.8 Risk Acceptance

Residual risks requiring acceptance shall be documented and approved by authorized management.

6.9 Third-Party Risk

Risks associated with vendors and third parties shall be evaluated.

6.10 Pre-Production Risk Assessment and Authorization

Before a new information system, application, cloud service, or material system capability is placed into production or authorized to process County information, Morgan County shall complete and document a formal risk assessment. The assessment shall be proportionate to the system's criticality, data sensitivity, connectivity, legal, contractual, CJIS, and privacy obligations, third-party dependencies, and potential business impact. Identified risks shall be treated or formally accepted, and written production authorization shall be approved by the Information Technology Director and the applicable system or data owner before go-live.

6.11 Significant Changes

Risk assessments shall be updated before implementing significant technology or business changes. Emergency changes shall follow the County's approved emergency-change process and receive a documented post-implementation risk review as soon as practical.

6.12 Documentation

Risk assessment activities and decisions shall be documented.

6.13 Annual Review

Formal risk assessments for production information systems shall be reviewed and refreshed at least annually. The overall Risk Assessment Program shall also be reviewed at least annually.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight.
- Approve significant risk acceptance decisions when appropriate.

7.2 County Leadership

- Support the Risk Assessment Program.
- Ensure departments participate in risk assessments.

7.3 Information Technology Director

- Administer the Risk Assessment Program.
- Coordinate enterprise risk assessments.
- Ensure required pre-production assessments and written production authorizations are completed.
- Maintain the County risk register.
- Ensure annual reviews are completed.

7.4 Department Heads

- Identify risks affecting departmental operations.
- Review and approve mitigation plans.
- Report significant changes affecting risk.

7.5 System Owners

- Identify system-specific risks.
- Approve production authorization and residual-risk acceptance for systems under their responsibility.
- Support vulnerability remediation.
- Validate mitigation activities.

7.6 Information Technology Staff

- Conduct technical assessments.
- Monitor vulnerabilities and threats.
- Document findings and recommend mitigations.

7.7 Supervisors

- Report operational risks.
- Support implementation of corrective actions.

7.8 Users

- Report suspected security weaknesses or risks.
- Comply with County security policies.

7.9 Contractors and Third Parties

- Cooperate with County risk assessments.
- Address contractual security requirements.
- Report risks affecting County information or systems.

8. Operational Procedures

8.1 Asset Identification

1. Identify information assets and business processes.
2. Assign asset owners.
3. Determine asset criticality.

8.2 Threat & Vulnerability Identification

1. Review threat intelligence and security advisories.
2. Identify known vulnerabilities through assessments and monitoring.
3. Document findings.

8.3 Risk Analysis

1. Evaluate likelihood and impact.
2. Assign an overall risk rating.
3. Document supporting rationale.

8.4 Risk Treatment

1. Select mitigation, transfer, acceptance, or avoidance.
2. Assign responsible parties.
3. Establish target completion dates.

8.5 Risk Register

1. Record identified risks in the County risk register.
2. Track mitigation progress.
3. Review open risks periodically.

8.6 Pre-Production Risk Assessment and Authorization

1. The system owner or sponsoring Department Head initiates the assessment before the planned production date or before County information is processed.
2. Document the system scope, owner, data sensitivity, criticality, connectivity, dependencies, applicable obligations, threats, vulnerabilities, likelihood, impact, and overall risk rating.
3. Document required safeguards, treatment actions, responsible parties, target dates, and residual risk.
4. Obtain written approval from the Information Technology Director and the applicable system or data owner before production use.
5. Record the production authorization, assessment date, approval evidence, and next annual review date in the designated County record or risk register.

8.7 Significant Changes

1. Refresh the applicable risk assessment before significant technology, process, or organizational changes are placed into production.
2. For emergency changes, document the post-implementation risk review and any corrective action as soon as practical.

8.8 Annual Risk Assessment Review

1. Review and refresh each production system's formal risk assessment at least annually.

2. Update risk ratings.
3. Document corrective actions and recommendations.

9. Compliance

Morgan County shall periodically assess compliance with this policy through internal reviews, management oversight, risk assessments, and authorized audits.

- A documented formal risk assessment and written production authorization shall be completed before each in-scope system, application, cloud service, or material system capability is placed into production or processes County information.
- Formal risk assessments shall be reviewed and refreshed at least annually and before significant changes are placed into production, subject to the documented emergency-change process.
- Risk treatment plans shall be documented and tracked.
- Risk acceptance decisions shall be documented and approved.
- Violations of this policy may result in disciplinary action.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Risk assessment reports
- Pre-production risk assessments and written production authorization records
- System inventory-to-risk-assessment coverage reports
- Risk register
- Vulnerability assessment results
- Risk treatment plans
- Risk acceptance approvals
- Third-party risk assessments
- Annual risk review documentation
- Corrective action tracking

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Risk Assessment (RA) and CA-6 Authorization controls
- National Institute of Standards and Technology (NIST) NIST SP 800-30 Guide for Conducting Risk Assessments
- National Institute of Standards and Technology (NIST) NIST SP 800-37 Rev. 2 Risk Management Framework
- Morgan County System and Information Integrity Policy (MCIT-007; Complete Policy, page 63)
- Morgan County Incident Response Policy (MCIT-008; Complete Policy, page 74)
- Morgan County Configuration Management Policy (MCIT-010; Complete Policy, page 93)

13. Revision History

Version	Date	Author	Description
1.0	July 21, 2026	Information Technology Director	Initial draft; pending approval
1.1	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

Risk Assessment Checklist

Complete	Task
☐	Assets identified
☐	Threats identified
☐	Vulnerabilities documented
☐	Likelihood assessed
☐	Impact assessed
☐	Overall risk rating assigned

Pre-Production Risk Assessment and Authorization Checklist

Complete	Task
☐	System, service, capability, and accountable owner identified
☐	Data sensitivity, CJI/PII status, criticality, connectivity, and dependencies documented

Complete	Task
☐	Applicable legal, contractual, CJIS, privacy, and security obligations identified
☐	Threats, vulnerabilities, likelihood, impact, and overall risk rating documented
☐	Required controls and risk-treatment actions documented
☐	Residual risk treated or formally accepted
☐	Information Technology Director and system or data owner approval recorded
☐	Production authorization date and next annual review date recorded

Risk Treatment Checklist

Complete	Task
☐	Treatment option selected
☐	Risk owner assigned
☐	Mitigation plan documented
☐	Target completion date established
☐	Progress tracked

Risk Acceptance Checklist

Complete	Task
☐	Residual risk documented
☐	Business justification provided
☐	Appropriate management approval obtained
☐	Acceptance recorded in risk register

Third-Party Risk Review Checklist

Complete	Task
☐	Vendor evaluated
☐	Security requirements reviewed
☐	Contractual protections verified
☐	Risk documented

Annual Risk Assessment Review Checklist

Complete	Task
☐	Production system inventory reconciled to formal risk assessments
☐	Each production system risk assessment reviewed and refreshed

Complete	Task
☐	Risk ratings and mitigation status updated
☐	Corrective actions and next review dates documented

Appendix – Recommended Records Retention

Maintain pre-production and annual risk assessments, production authorizations, risk registers, vulnerability assessment reports, treatment plans, risk acceptance approvals, significant-change and emergency-change reviews, third-party risk assessments, and annual review documentation in accordance with County retention schedules and CJIS requirements.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or changes to applicable laws, CJIS requirements, or NIST guidance. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Risk Management	Sections 6–8
NIST RA-3 Risk Assessment	6.1–6.6, 8.1–8.3
NIST RA-5 Vulnerability Monitoring and Scanning	6.4, 8.2
NIST RA-7 Risk Response	6.7–6.8, 8.4–8.5
NIST RA-9 Criticality Analysis	6.2, 8.1
NIST CA-6 Authorization	6.10, 8.6, 9

Morgan County Acceptable Use Policy & Procedures

Document Number: MCIT-013

Version: 3.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Overview
- 2. Purpose
- 3. Scope
- 4. Individual Responsibilities
- 5. Internet and Email
- 6. General Use Ownership
- 7. Blogging and Social Media
- 8. Security and Proprietary Information
- 9. Unacceptable Use
- 10. Roles and Responsibilities
- 11. Operational Procedures
- 12. Compliance
- 13. Exceptions
- 14. Audit Evidence
- 15. References
- 16. Revision History
- Appendices

1. Overview

This Acceptable Use Policy governs the use and security of all information and computer equipment from Morgan County. It also covers the use of email, the internet, voice, and mobile computing equipment.

This policy applies to all information, in any form, relating to the activities of Morgan County, and to all information processed by the County about other organizations with which it deals.

This policy also covers all IT and information communication facilities operated by or on behalf of Morgan County.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the County. These systems are to be used for business purposes in serving the interests of the County during normal operations.

Morgan County is committed to protecting its employees, partners, and the County from illegal or damaging actions by individuals, either knowingly or unknowingly.

It is the responsibility of every County technology user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Morgan County. These rules are in place to protect the employee and the County. Inappropriate use exposes the County to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to employees, contractors, consultants, temporary workers, and other workers of Morgan County, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by the County.

It also applies to the use of information, electronic and computer equipment, and network resources to conduct business activities or interact with internal networks and business systems, whether owned or leased by Morgan County, the employee or a third party.

All employees, contractors, consultants, temps, and other workers of Morgan County are responsible for exercising judgment with respect to the appropriate use of information, electronic devices, and network resources in accordance with Morgan County policies and standards and local laws and regulations.

4. Individual Responsibilities

Access to the Morgan County IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the County IT systems using their IDs.

Individuals must not:

- Allow anyone else to use their user ID and password on any Morgan County IT system.
- Leave their user accounts logged in at an unattended or an unlocked computer.
- Use someone else's user ID and password to access Morgan County's IT systems.

- Leave their password unprotected (for example writing it down and leaving it under your keyboard).
- Perform any unauthorized changes to Morgan County's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-Morgan County authorized device to the Morgan County network or IT systems. The "MorganPublic" wireless network is provided for personal equipment and visitors. The same code of conduct is required while using this service but can be used for any legal purpose.
- Store Morgan County data on any non-authorized Morgan County equipment.
- Employees must not give or transfer Morgan County data or software to any person or organization outside Morgan County without authorization from the appropriate elected official or department head, except through an authorized disclosure under the Utah Government Records Access and Management Act (GRAMA) or other applicable law.

Department heads must ensure that individuals receive clear directives on the extent and limits of their authority over computer systems and data.

5. Internet and Email

The use of the internet and email of Morgan County is intended for professional purposes. Personal use is permitted when it does not affect the individual's professional performance, does not in any way harm Morgan County, does not violate any terms and conditions of employment and does not place the individual or the County in violation of legal or other obligations. All individuals are therefore responsible for their actions on the internet as well as when using email systems.

Individuals must not:

- Use the internet or email for harassment or abuse.
- Use obscene, threatening, discriminatory, harassing, or abusive communications.
- Access, upload, send or receive data (including images) that Morgan County considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material.
- Use email systems in a way that could affect their reliability or efficiency, for example by distributing chain letters or spam.
- Send sensitive or confidential information that is not encrypted to the outside world.
- Use of unsolicited email originating from within Morgan County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Morgan County or connected via Morgan County's network.
- Make official commitments by internet or email on behalf of Morgan County, unless authorized to do so.

- Download copyrighted material such as music media files (MP3), films and videos (non-exhaustive list) without appropriate approval.
- In any way, violate copyright, database rights, trademarks, or other intellectual property rights.
- Download any software from the internet without the prior consent of the Information Technology Department.

6. General Use Ownership

- Morgan County's proprietary information stored on electronic and computing devices whether owned or leased by Morgan County, remains the sole property of Morgan County. You must ensure through legal or technical means that proprietary information is protected in accordance with the data protection standards.
- You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Morgan County proprietary information.
- You may access, use, or share Morgan County's proprietary information only to the extent it is authorized and necessary to perform the tasks assigned to you.
- Employees are responsible for exercising their good judgment as to the reasonableness of personal use. It is the responsibility of each department to develop guidelines for the personal use of internet/intranet/extranet systems. In the absence of such policies, employees should be guided by their department's policies on personal use and, in the event of uncertainty, should consult their supervisor or manager.
- Morgan County reserves the right to monitor, audit, inspect, and review County systems, networks, devices, accounts, and communications to ensure compliance with County policies and applicable law. Users should have no expectation of privacy in any communication, data, file, internet usage, email, text message, or information created, stored, transmitted, or received using County systems.

7. Blogging and Social Media

- Employees' use of blogs, social media platforms, social networking sites, online forums, discussion boards, podcasts, video-sharing platforms, and similar online communications is subject to the terms and restrictions of this policy.
- Limited and occasional personal use of Morgan County systems to access or participate in such online communications is permitted, provided the use is lawful, professional, responsible, does not violate County policy, does not interfere with the employee's job duties or productivity, does not consume excessive County resources, and is not contrary to the interests of Morgan County.
- Employees shall not use social media or other online communications in a manner that could reasonably be expected to harm the reputation, operations, or interests of Morgan County, disclose confidential or protected information, or create the appearance that

personal opinions are being expressed on behalf of Morgan County unless authorized to do so.

- All use of Morgan County systems, including access to blogs, social media platforms, and other online communications, may be monitored and reviewed in accordance with County policy and applicable law.
- Employees shall not engage in social media activity, online communications, or other electronic communications that may reasonably be expected to harm the reputation, operations, or interests of Morgan County. Employees are also prohibited from making discriminatory, defamatory, harassing, threatening, or otherwise unlawful statements through social media platforms, blogs, online forums, discussion boards, podcasts, video-sharing platforms, or similar online communications.
- Employees may also not attribute personal statements, opinions or beliefs to Morgan County when engaged in said communications.

8. Security and Proprietary Information

- All access to Morgan County's computer network must be protected by passwords.
- It is prohibited to allow access to another person, either deliberately or by failing to adequately protect the right of access that has been granted.
- Messages posted by employees from a Morgan County email address on forums should contain a warning that the opinions expressed are strictly theirs and not necessarily those of Morgan County, unless the message is posted in the course of professional duties.
- Employees must exercise extreme caution when opening attachments to emails received from unknown senders, which may contain malware.
- Employees must not remove or disable anti-virus software.
- Employees must not attempt to remove virus-infected files or clean up an infection, other than using approved Morgan County anti-virus software and procedures.

8.1 Mobile Storage Devices

Mobile devices such as USB flash drives, CDs, DVDs, and removable hard drives should only be used when network connectivity is not available or there is no other secure method of data transfer. Only authorized Morgan County mobile storage devices with encryption enabled should be used when transferring sensitive or confidential data.

8.2 Software

Employees are required to utilize only software authorized by Morgan County on the County's computers. This includes, but is not limited to, the primary systems and applications supported by the County, such as Microsoft Windows and Microsoft 365 (Word, Excel, and related tools). Authorized software must be utilized in accordance with the

software supplier's licensing agreements. All installations must be approved and executed by the Morgan County Information Technology Department.

Employees may use only artificial intelligence tools and services authorized by Morgan County. Microsoft Copilot, when accessed using an official County-issued account protected by enterprise data protection, is approved for standard AI chat purposes on County computers.

Any other artificial intelligence product, service, feature, or account requires prior written approval from the Information Technology Director using the County's AI Tool Use Request and Approval Form. The request must identify the proposed business purpose, requested users, intended information use, account or licensing level, and anticipated duration of use. The request must be approved by the applicable Department Head, Director, or Elected Official before submission to Information Technology.

Approval applies only to the tool, account, users, and business purpose identified in the request. The Information Technology Director may impose conditions, require additional review, suspend or revoke approval, or require a new request when the product, vendor terms, information use, or business purpose materially changes. Personal or free AI accounts may not be used for County business unless expressly approved in writing.

All approved AI use remains subject to County requirements concerning acceptable use, confidentiality, information security, records retention, intellectual property, and lawful use.

9. Unacceptable Use

The following activities are prohibited. Under no circumstances is an employee of Morgan County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing County-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Infringements of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or by similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" products or other software the use of which is not authorized by Morgan County.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Morgan County or the end user holds no active license is strictly prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Making fraudulent offers of products, items, or services originating from any Morgan County account.
- Making security breaches or disruptions of network communication.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

10. Roles and Responsibilities

- **County Commission:** Approve major policy revisions and provide executive oversight.
- **Information Technology Director:** Administer this policy, approve exceptions, oversee monitoring and enforcement.
- **Department Heads:** Ensure employees understand and comply with this policy.
- **Supervisors:** Address misuse and ensure acknowledgements are completed.
- **Authorized Users:** Use County resources responsibly and report security incidents.
- **Information Technology Department:** Manage accounts, software approvals, monitoring, and investigations.

11. Operational Procedures

- Provide each user with this policy before or immediately after system access is granted.
- Obtain a signed acknowledgement from each authorized user.
- Approve all software installations through the Information Technology Department.
- Investigate suspected policy violations and document findings.
- This policy and its procedures shall be reviewed at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving unauthorized access to Criminal Justice Information (CJI) or systems used to process, store, or transmit CJI, or changes to applicable laws, Criminal Justice Information Services (CJIS) requirements, or National Institute of Standards and Technology (NIST) guidance. Significant revisions require approval by the Morgan County Commission.

12. Compliance

Compliance with this policy is mandatory. Violations may result in one or more of the following: disciplinary action, loss of access privileges, civil liability, or criminal prosecution.

13. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

14. Audit Evidence

- Signed policy acknowledgements
- Training records
- Software approval records
- System audit logs
- Incident reports
- Annual policy review records

15. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5
- Morgan County MCIT-001 through MCIT-015 policies (Complete Policy, Table of Contents, page 1)

16. Revision History

Version	Date	Author	Description
2.1	August 19, 2025	Morgan County	Version 2.1 adopted (CR 25-38)
3.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; AI tool request and approval process added; pending approval

Appendices, Forms & Checklists

Appendix A – Acceptable Use Acknowledgement

I acknowledge that I have received a copy of the Morgan County Acceptable Use Policy. I have read and understand the policy. I understand that, if I violate the policy, I may be subject to

disciplinary action, including termination. I further understand that I will contact my supervisor if I have any questions about any aspect of the policy.

Employee Name	
Department	
Signature	
Date	
Supervisor	
IT Verification	

Appendix B – New User Checklist

Complete	Task
☐	Policy provided
☐	Acknowledgement signed
☐	Training completed
☐	Account created

Appendix C – Software Approval Checklist

Complete	Task
☐	Business need documented
☐	IT approval
☐	License verified
☐	Installed by IT

Appendix D – AI Usage Checklist

Complete	Task
☐	Approved AI tool or documented approval used
☐	AI request form retained when required
☐	No CJIS entered
☐	Enterprise or IT-approved account used

Appendix E – Policy Violation Checklist

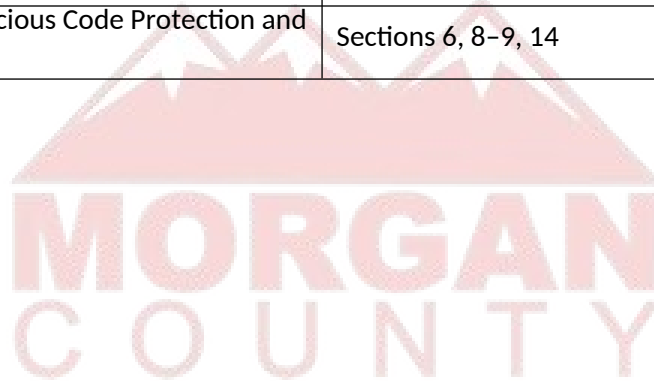
Complete	Task
☐	Incident documented
☐	Evidence preserved
☐	Management notified
☐	Corrective action completed

Appendix F – Annual Policy Review Checklist

Complete	Task
☐	Policy reviewed
☐	Technology changes reviewed
☐	Legal changes reviewed
☐	Commission approval if revised

Appendix G – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Rules of Behavior and Acceptable Use	Sections 1-12
NIST PL-4 / PS-6 Rules of Behavior and Access Agreements	Sections 1-4, 10-12; Appendix A
NIST AC-2 / AC-3 / AC-6 Account and Access Controls	Sections 4, 6, 8-9
NIST CM-7 Least Functionality	Sections 5, 8.2, 9, 11
NIST MP-7 Media Use	Sections 8.1, 9
NIST SI-3 / SI-4 Malicious Code Protection and System Monitoring	Sections 6, 8-9, 14



Morgan County Remote Work Policy & Procedures

Document Number: MCIT-014

Version: 2.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Policy Statement
- 2. Purpose
- 3. Scope
- 4. Risks
- 5. Equipment
- 6. User Responsibility
- 7. Remote and Mobile Working Arrangements
- 8. Access Controls
- 9. Antivirus Protection
- 10. Policy Acknowledgement
- 11. Roles and Responsibilities
- 12. Operational Procedures
- 13. Compliance
- 14. Exceptions
- 15. Audit Evidence
- 16. References
- 17. Revision History
- Appendices

1. Policy Statement

Morgan County may provide authorized users with County-approved equipment, secure access, and the opportunity to work remotely when operationally appropriate. Remote work is discretionary and must comply with this policy and all other applicable County policies.

2. Purpose

The purpose of this document is to state the Remote Working policy of Morgan County.

Portable computing devices are provided to assist users to conduct official business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognized as valuable organizational information assets, and safeguarded appropriately.

3. Scope

This document applies to all employees of Morgan County and contractual third parties who use Morgan County IT facilities and equipment remotely, or who require remote access to Morgan County Information Systems or information.

This policy should always be adhered to whenever any user makes use of portable computing devices. This policy applies to all users of Morgan County IT equipment and personal IT equipment when working away from Morgan County offices/facilities.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Desktop Computers.
- Mobile phones.
- Wireless technologies.
- Remote Terminal Access.

4. Risks

Morgan County recognizes that there are risks associated with users accessing and handling information to conduct official work. The mobility, technology and information that make portable computing devices and remote access terminals so useful to employees and organizations also make them valuable assets for thieves.

This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss, or theft.
- Accidental or deliberate overlooking by unauthorized individuals.
- Unauthorized access to PROTECTED and RESTRICTED information.
- Unauthorized introduction of malicious software and viruses.
- Potential sanctions against the County imposed by the authorities because of information loss or misuse.
- Potential legal action against the County because of information loss or misuse.
- Morgan County reputational damage because of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of Morgan County and may result in financial loss and an inability to provide necessary services to the public.

5. Equipment

All IT equipment (including portable computer devices) supplied to users is the property of Morgan County. It must be returned upon the request of Morgan County. Access for support shall be provided to Morgan County Information Technology Staff to allow essential maintenance, security work, or removal upon request.

The Information Technology Director may require the return or reassignment of County-owned equipment when it has not been used for authorized County business for ninety (90) consecutive calendar days, is no longer operationally necessary, or is otherwise not being used for its assigned purpose. The ninety-day non-use period does not include approved leave, seasonal assignments, emergency or continuity equipment, or another documented exception approved by the Information Technology Director. Users shall return County-owned equipment by the deadline stated in the request. If no deadline is stated, the equipment shall be returned within two County business days. Information Technology may require same-day return when continued possession presents a documented security or operational risk, coordinated with Human Resources and the applicable Department Head, Director, or Elected Official.

All IT equipment will be supplied and installed by Morgan County Information Technology Staff. Hardware, software, and remote terminal access must only be provided by Morgan County Information Technology Staff.

6. User Responsibility

It is the user's responsibility to ensure that the following points are always adhered to:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on a Morgan County owned portable computer device.
- Users will not install any screen savers on a Morgan County owned portable computer device.
- Users will not change the configuration of any Morgan County owned portable computer device.
- Users will not install any hardware to or inside any Morgan County owned portable computer device, unless authorized by Morgan County Information Technology Department.
- Users will allow the installation and maintenance of Morgan County installed Antivirus updates immediately.
- County-owned portable computers assigned for regular use shall be powered on and connected to the internet or County network at least once every seven calendar days for sufficient time to receive security updates and management instructions. Users shall complete required restarts promptly. Approved leave, emergency or continuity equipment,

and other documented exceptions may follow an Information Technology-approved schedule.

- Business critical data should be stored on a Morgan County file and print server wherever possible and not held on the portable computer device.
- Users must not remove or deface any asset registration number.
- User requests for hardware or software upgrades must be approved by the Information Technology Department. Equipment and software will then be purchased and installed by Information Technology Staff.
- Only software supplied and approved by Morgan County can be used (e.g. Word, Excel, Adobe, etc.).
- County-owned equipment shall be used only by the authorized County user to whom it is assigned. No other person—including non-employees, household members, family members, friends, or guests—may use the equipment unless the Information Technology Director has expressly authorized the use for a legitimate County business purpose.
- Use of artificial intelligence tools while working remotely is governed by MCIT-013 Acceptable Use Policy (Complete Policy, page 125). Only County-approved tools, services, accounts, and authorized information uses are permitted.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Morgan County may recover the costs of repair.
- Morgan County may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

7. Remote and Mobile Working Arrangements

Remote work is a discretionary privilege and not an entitlement. The Information Technology Director may suspend or revoke remote-work authorization when a user fails to comply with this policy, another applicable County policy, security requirements, or the conditions of an approved remote-work arrangement. The Information Technology Director shall coordinate with Human Resources and the user's applicable supervisory authority—whether a Department Head, Director, or Elected Official—when the action affects the user's work assignment or may result in disciplinary action.

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interest of a thief. When working at home, the work area should be kept separate from the remainder of the residence where reasonably practicable. Equipment must be secured whenever it is not in use.

Users must ensure that access / authentication tokens and personal identification numbers are always kept in a separate location to the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorized people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use.

Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Paper containing PROTECTED or RESTRICTED information shall be shredded using an approved method or placed in a County-approved secure-destruction container for disposal in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47).

8. Access Controls

It is essential that access to all PROTECTED or RESTRICTED information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Users shall not share passwords, PINs, MFA factors, or screen-unlock credentials. Information Technology shall maintain approved administrative recovery mechanisms or device-recovery keys sufficient to recover, reset, lock, or wipe County-owned equipment without obtaining or retaining the user's authentication credential.

All County-owned portable devices shall use full-device encryption. Criminal Justice Information (CJI) and all PROTECTED or RESTRICTED data stored on portable devices shall be encrypted at rest without exception using County-approved cryptographic mechanisms. CJI transmitted outside a physically secure location shall use Federal Information Processing Standards (FIPS) 140-3 certified cryptographic modules or FIPS-validated Advanced Encryption Standard (AES) with a symmetric key of at least 128-bit strength, as required by Criminal Justice Information Services (CJIS).

Remote access over public or external networks shall use a County-approved, centrally managed VPN or equivalent encrypted access service and MFA. Cryptography protecting CJI shall meet current CJIS requirements and shall be configured and validated by the Information Technology Department.

8.1 Mobile Device Management for CJI

County-owned mobile devices used for direct access to CJI shall be enrolled in a centrally administered Mobile Device Management (MDM) solution before access is granted. The MDM solution shall:

- Support remote locking and remote wiping of the device.
- Set and lock device configurations and enforce mandatory County security settings.
- Detect rooted or jailbroken devices, unauthorized configurations, and unauthorized software or applications.

- Enforce full-device or approved container encryption and restrict CJI to authorized applications and storage areas.
- Determine the location of agency-controlled devices when required for security or recovery.
- Prevent unpatched or noncompliant devices from accessing CJI or CJI systems.
- Automatically wipe the device after the County-defined number of failed access attempts.

Devices with unauthorized changes shall not process, store, or transmit CJI. An MDM exception for indirect-access systems is permitted only after the CJIS Systems Officer (CSO) determines that access is indirect under CJIS requirements.

9. Antivirus Protection

The Morgan County Information Technology Department will deploy Antivirus to all Windows devices. There must be no attempt to remove or disable the Antivirus software and the device **must** be rebooted when said Antivirus software requests that it do so.

10. Policy Acknowledgement

If any user is found to have breached this policy, they may be subject to Morgan County's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

I understand and agree to the above.

EMPLOYEE

COUNTY

Authorized Signature

Authorized Signature

Print Name and Title

Print Name and Title

11. Roles and Responsibilities

- **County Commission:** Provide executive oversight and approve major policy revisions.
- **Information Technology Director:** Administer the Remote Work Program; approve exceptions; suspend or revoke remote-work authorization for policy or security violations; and recall or reassign County equipment that is unused for ninety (90) consecutive calendar days or is no longer operationally necessary.
- **Department Heads:** Approve remote work requests and ensure employee compliance.
- **Information Technology Department:** Deploy, secure, maintain, and monitor remote access technologies.
- **Users:** Protect County equipment and information while working remotely.

12. Operational Procedures

- Submit remote work request.
- Information Technology Staff provision equipment and VPN/MFA.
- Verify endpoint protection before remote access.
- Review remote access and this policy at least annually and following assessment or audit findings, significant system or operating-environment changes, security incidents or breaches involving CJI, or changes to CJIS or National Institute of Standards and Technology (NIST) guidance.

13. Compliance

Compliance with this policy is mandatory.

14. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the Terminal Agency Coordinator (TAC) and Local Agency Security Officer (LASO) and submitted for CJIS Systems Officer (CSO) approval when required by the CJIS compensating-control process.

15. Audit Evidence

- Remote work approvals
- VPN logs
- Device inventory
- MFA records
- Training records
- MDM compliance and remote wipe test reports
- FIPS cryptographic module or algorithm validation records

16. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5
- MCIT-013 Acceptable Use Policy (Complete Policy, page 125)

17. Revision History

Version	Date	Author	Description
1.2	2024	Morgan County	Prior policy; adopted 8/19/2025 (CR 25-46)
2.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; remote-work safeguards and equipment-return procedures updated; pending approval

Appendices, Forms & Checklists

Appendix A – Remote Work Approval Checklist

Complete	Task
☐	Manager approval
☐	IT approval
☐	Equipment assigned
☐	VPN configured
☐	MFA verified

Appendix B – Remote Work Security Checklist

Complete	Task
☐	Device encrypted
☐	Antivirus current
☐	Documents secured
☐	Screen lock enabled
☐	MDM enrollment verified for direct CJI access
☐	Remote lock and wipe tested
☐	Root/jailbreak detection enabled
☐	Patch compliance verified

Appendix C – Annual Remote Access Review

Complete	Task
☐	User access reviewed
☐	Equipment inventory verified
☐	Policy reviewed

Appendix D – CJIS & NIST Control Mapping

Control	Policy Section
CJIS Remote Access and Mobile Devices	Sections 3–12
NIST AC-17 / IA-2(1) / IA-2(2) Remote Access and MFA	Sections 7–8.1, 11–12
NIST PE-17 Alternate Work Site	Sections 4, 6–8
NIST SC-8(1) / SC-13 / SC-28(1) Cryptographic Protection	Sections 4, 7–8.1
NIST CM-6 / CM-7 Configuration Settings and Least Functionality	Sections 5–6, 9, 12
NIST SI-3 Malicious Code Protection	Sections 4, 6, 9, 12
NIST AC-19 / AC-7(2) / CM-6 Mobile Device Management	Sections 5–8.1, 12



Morgan County Contingency Planning, Backup & Disaster Recovery Policy & Procedures

Document Number: MCIT-015

Version: 1.0 Draft

Policy Owner: Morgan County Information Technology Department

Review Cycle: Annual

Table of Contents

- 1. Purpose
- 2. Authority
- 3. Scope
- 4. Objectives
- 5. Definitions
- 6. Contingency Planning, Backup & Disaster Recovery Policy
- 7. Roles and Responsibilities
- 8. Operational Procedures
- 9. Compliance
- 10. Exceptions
- 11. Audit Evidence
- 12. References
- 13. Revision History
- Appendices

1. Purpose

Establish requirements for contingency planning, backup, disaster recovery, and reconstitution so Morgan County can protect information and resume essential services after disruption, compromise, or failure within approved recovery objectives.

2. Authority

Supports the FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 Contingency Planning (CP) controls, applicable Utah law, records-retention requirements, and Morgan County information security policies.

3. Scope

Applies to County information systems, Criminal Justice Information (CJI), essential business data, Hyper-V virtual machines, Microsoft 365 services, network infrastructure, backup repositories, system documentation, and personnel or service providers assigned backup or recovery responsibilities.

4. Objectives

Maintain encrypted and recoverable backup copies, protect backups from unauthorized change or destruction, verify backup integrity, test recovery, document alternate processing and communications dependencies, and restore essential County services in an approved order within a 24-hour Recovery Point Objective and 24-hour Recovery Time Objective.

5. Definitions

- **Contingency Plan:** Documented roles, priorities, resources, communications, and procedures used to sustain or restore essential services after a disruption.
- **Immutable Backup:** A backup copy protected from alteration or deletion for a defined retention period.
- **Recovery Point Objective (RPO):** The maximum approved period of data loss measured backward from a disruption. Morgan County's formal RPO is 24 hours unless a system-specific plan establishes a shorter value.
- **Recovery Time Objective (RTO):** The maximum approved time to restore an essential service after a disruption. Morgan County's formal RTO is 24 hours unless a system-specific plan establishes a shorter value.
- **Reconstitution:** Returning a recovered system to a fully operational and monitored known state after temporary recovery activities are complete.
- **Restore Test:** A controlled recovery of backup information used to verify that data can be retrieved, decrypted, mounted, started, and validated.

6. Contingency Planning, Backup & Disaster Recovery Policy

The following requirements establish Morgan County's minimum contingency planning, backup, recovery, and reconstitution controls.

6.1 Recovery Objectives and Service Priorities

The County shall use a formal RPO of no more than 24 hours and an RTO of no more than 24 hours for systems covered by this policy. More frequent backups provide additional recoverability but do not change the approved objective unless documented. Critical systems, dependencies, owners, recovery order, and any shorter objectives shall be identified through business impact and risk analysis.

6.2 Contingency Plan Content and Coordination

The contingency plan shall identify essential mission and business functions, critical assets and data, recovery roles, contacts, escalation paths, system dependencies, alternate storage and processing arrangements, telecommunications needs, required credentials and documentation, recovery steps, and return-to-service criteria. It shall be coordinated with incident response, continuity of operations, emergency management, physical security, and departmental continuity plans.

6.3 Hyper-V Virtual Machine Backups

Operational Hyper-V virtual machines and the system information needed to restore them shall be backed up at least every four hours to protected storage on a local Windows Server. At least daily, encrypted immutable copies shall be maintained on a local network-attached storage system and on a geographically separate offsite immutable storage system. Virtual machine backups shall be retained for at least six months unless legal, records, or system-specific requirements require longer retention.

6.4 Microsoft 365 Backups

The Microsoft 365 Government G3 tenant shall be backed up nightly to the local UniFi network-attached storage system. Backup snapshots shall be encrypted, immutable, and retained for one year. Because the current Microsoft 365 backup is stored locally, the Information Technology Director shall document and review at least annually whether an additional offsite or otherwise independent protected copy is required based on risk, service criticality, and recovery objectives.

6.5 Backup Protection and Administrative Access

All backup data shall be encrypted in transit and at rest using approved cryptographic mechanisms. All accounts, including backup, storage, cloud, and administrative accounts, shall use multi-factor authentication. Backup access shall be limited to authorized personnel, use least privilege, and protect recovery credentials, cryptographic keys, configuration information, and system documentation from unauthorized disclosure or modification.

6.6 Alternate Storage and Processing Capability

The County shall establish an alternate storage site, including necessary agreements, that is sufficiently separated from the primary site, permits timely retrieval, and provides security and availability controls equivalent to the primary site. The offsite immutable backup repository serves as the current alternate storage site. Area-wide accessibility risks shall be

identified with explicit mitigation actions, such as alternate electronic access methods or an additional protected recovery source.

The County shall designate at least one geographically separated alternate processing location or authorized processing service capable of resuming essential functions within the RTO. Necessary internal authorizations or provider agreements shall address transfer and resumption, required equipment and supplies or timely delivery, equivalent security controls, accessibility risks and mitigations, and priority of service. The current recovery method may use acquisition or repurposing of a compatible Windows Server host capable of running Hyper-V when documented capacity, licensing, networking, delivery, secure access, and service-priority arrangements can meet the 24-hour RTO. A permanently powered standby server is not required when these documented arrangements meet the control requirements.

6.7 Backup Monitoring and Daily Integrity Verification

Backup jobs and the automated backup-integrity verification service shall operate daily and generate notifications for success, failure, and conditions requiring action. Alerts shall be delivered to the Information Technology Director and designated Information Technology staff 24 hours a day. IT shall review backup and integrity notifications as they are received and perform a documented routine review each County business morning. Failures that could cause an RPO or RTO breach shall be investigated, corrected, and escalated without unreasonable delay.

6.8 Monthly Restore Testing

At least once each calendar month, IT shall perform and document a full virtual-machine restore and boot test on a rotating basis. Tests shall use protected local and offsite copies over time, occur in an isolated or otherwise access-restricted recovery environment, and verify decryption, retrieval, boot, application availability, representative data, and authorized logon. The rotation shall provide risk-based coverage of critical virtual machines and recovery sources, and failed tests shall produce tracked corrective actions.

6.9 Contingency Training and Annual Exercise

Personnel assigned contingency responsibilities shall receive role-appropriate training within 30 days of assuming the role, when required by system changes, and annually thereafter. Training content shall be reviewed and updated at least annually and following an incident involving unauthorized access to CJI or a system used to process, store, or transmit CJI, or following a contingency simulation or exercise. Participation in an exercise and its lessons-learned session may satisfy applicable role training.

The County shall test the contingency plan at least annually using a checklist review, walk-through, tabletop, simulation, or more comprehensive exercise coordinated with related plans. Results, lessons learned, responsible parties, due dates, and corrective actions shall be documented.

6.10 Network and Telecommunications Recovery

The County shall establish alternate voice and data telecommunications services, including necessary agreements, capable of resuming essential operations within the RTO when primary services are unavailable at primary or alternate sites. Primary and alternate service arrangements shall address priority of service in accordance with availability requirements. The County shall request Telecommunications Service Priority when eligible and required for national security emergency preparedness services. Alternate services shall be selected and documented to reduce shared facilities, carriers, paths, or other single points of failure.

Critical communications and network dependencies shall be documented and prioritized for recovery. The County shall maintain a backup UniFi Enterprise Fortress Gateway and back up gateway settings to the UniFi cloud at least weekly. Recovery procedures shall include activating approved alternate telecommunications when needed, restoring the approved gateway configuration, validating internet and internal connectivity, and confirming that required segmentation, remote-access, firewall, threat-management, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), logging, and notification controls are active before normal service resumes.

6.11 Recovery and Reconstitution

Recovery shall be authorized and coordinated with incident response when compromise is suspected. IT shall select a known-good recovery point, preserve evidence when required, restore services in the approved order, validate security and data integrity, reestablish monitoring and logging, obtain system-owner acceptance, and return systems to production only after defined criteria are met. Temporary recovery capabilities shall be securely removed or normalized during reconstitution.

6.12 Transaction and Data Reconciliation

For transaction-based systems, recovery procedures shall restore the most recent consistent point within the approved RPO and use supported logs, application functions, source records, or manual reconciliation to recover or account for transactions after that point. The applicable system or data owner shall validate business completeness before final return to service.

6.13 Retention and Secure Disposal

Backup retention shall meet this policy, approved County schedules, legal holds, records requirements, and CJIS requirements. Expired backup information and retired backup media shall be securely disposed of or sanitized in accordance with MCIT-005 (Complete Policy, page 47). Changes to backup retention or immutability settings require authorization and documentation.

6.14 Plan Review and Maintenance

This policy, the contingency plan, recovery procedures, system priorities, contact information, and recovery dependencies shall be reviewed at least annually and after significant system or staffing changes, exercises, failed restore tests, audit findings, or actual disruptions or security incidents. Approved updates shall be communicated to personnel with contingency responsibilities.

7. Roles and Responsibilities

7.1 County Commission

- Provide executive oversight and support resources proportionate to continuity risk.
- Approve major policy revisions.

7.2 County Leadership and System Owners

- Identify essential functions, critical information, dependencies, service priorities, and acceptable recovery impacts.
- Participate in annual contingency exercises and validate recovered business services and data.

7.3 Information Technology Director

- Own and maintain the contingency, backup, recovery, and reconstitution program.
- Approve recovery priorities, backup schedules, access, exceptions, test scope, and corrective actions.
- Coordinate CJJ-related requirements with the Terminal Agency Coordinator (TAC), Local Agency Security Officer (LASO), and CJIS Systems Officer (CSO) when applicable.
- Report material recovery risks, failed tests, and unmet objectives to County leadership.

7.4 Information Technology Staff

- Operate and monitor backup jobs, immutable repositories, integrity checks, and notifications.
- Perform documented monthly restore tests and annual contingency exercises.
- Maintain recovery documentation, protected credentials, configurations, evidence, and corrective-action records.
- Maintain alternate-storage, alternate-processing, and alternate-telecommunications arrangements and supporting agreements.
- Execute authorized recovery and reconstitution activities and escalate material failures.

7.5 Department Heads and Data Owners

- Identify departmental records, applications, and manual workarounds required for continuity.
- Assist with business validation, transaction reconciliation, and prioritization during recovery.
- Notify IT of system, service, or records changes that affect backup and recovery requirements.

7.6 Service Providers

- Meet documented County backup, availability, security, incident notification, and recovery requirements applicable to the service.
- Provide recovery assistance and evidence when required by contract or County direction.

8. Operational Procedures

8.1 Routine Backup Operations

1. Maintain a current inventory of protected systems, data, owners, dependencies, backup schedules, retention, and recovery priority.
2. Configure Hyper-V backups for the local four-hour operational schedule and daily immutable local and offsite copies.
3. Configure nightly Microsoft 365 tenant backups and weekly gateway-configuration backups.
4. Confirm encryption, immutability, multi-factor authentication, notifications, retention, and authorized access are enabled.

5. Record approved changes to jobs, repositories, credentials, or retention settings.

8.2 Business-Morning Verification

1. Review backup completion notifications and the automated integrity-verification result each County business morning.
2. Identify failed, missed, incomplete, unexpectedly small, or otherwise abnormal jobs and confirm repository availability.
3. Correct the condition, rerun the affected job when appropriate, and verify successful completion.
4. Document failures and corrective actions that are material, recurring, or could affect an approved recovery objective.

8.3 Monthly Full Virtual-Machine Restore Test

1. Select a full virtual machine according to the approved rotation and identify the source repository and recovery point.
2. Restore the virtual machine to an isolated or access-restricted Hyper-V test environment without disrupting production.
3. Verify decryption, retrieval, boot, application availability, representative data, authorized login, and expected security controls.
4. Record elapsed recovery time, recovery point, results, evidence, tester, date, and any corrective actions.
5. Securely remove or reset the test instance after evidence is retained and the test is complete.

8.4 Incident Recovery and Reconstitution

1. Authorize recovery, identify the incident lead, and coordinate with the incident-response process when compromise is suspected.
2. Contain affected systems, preserve required evidence, and identify a known-good recovery point.
3. Restore required network, identity, host, and security services before dependent applications.

4. Restore virtual machines and data in approved priority order and reconcile transactions or source records as needed.
5. Validate data, applications, access, encryption, segmentation, endpoint protection, monitoring, logging, and notifications.
6. Obtain applicable system-owner acceptance, authorize return to service, and document actual RPO and RTO performance.
7. Reconstitute the environment, remove temporary capabilities, conduct lessons learned, and track corrective actions.

8.5 Annual Contingency Exercise

1. Select an exercise scenario that addresses a realistic disruption, compromise, or site failure affecting essential services.
2. Include responsible IT personnel, applicable leadership and system owners, and related incident or continuity functions.
3. Exercise notifications, decisions, alternate storage access, alternate processing, communications recovery, restoration priorities, and validation steps.
4. Document results, lessons learned, assigned corrective actions, due dates, and closure evidence.

8.6 Microsoft 365 Recovery

1. Verify the requested recovery is authorized and determine the required user, mailbox, file, site, or tenant recovery point.
2. Restore from the protected UniFi Network-Attached Storage (NAS) backup using the least disruptive supported method.
3. Validate recovered content with the authorized owner and document the request, recovery point, result, and exceptions.

8.7 Gateway and Communications Recovery

1. Determine whether the outage affects the gateway, the telecommunications provider or path, or both.
2. Activate approved alternate telecommunications service when primary voice or data service is unavailable.

3. Activate the backup Enterprise Fortress Gateway when the primary gateway cannot be recovered within the required timeframe.
4. Restore the latest approved weekly configuration backup from UniFi cloud.
5. Validate external and internal connectivity, segmentation, VPN or remote access, firewall rules, threat management, IDS/IPS, logging, and alerts before normal service resumes.

8.8 Corrective Actions

1. Create a corrective action for failed backups, failed integrity checks, failed restore tests, missed objectives, or exercise findings that create material risk.
2. Assign an owner and due date based on risk and track the action to verified closure.
3. Update procedures, training, architecture, schedules, or resources when lessons learned identify a needed change.

9. Compliance

Morgan County shall periodically assess compliance with this policy through backup and integrity records, access reviews, restore-test evidence, contingency exercises, risk reviews, management oversight, and authorized audits.

- Required backups, encryption, immutability, multi-factor authentication, monitoring, and retention shall remain enabled and effective.
- Monthly restore testing and annual contingency testing shall be completed and documented.
- Material failures, missed recovery objectives, and open corrective actions shall be reported and managed based on risk.
- Violations may result in access restriction, corrective action, disciplinary action, contract remedies, or other measures permitted by law and County policy.

10. Exceptions

Exceptions require written approval from the Information Technology Director and the applicable Department Head or system owner, with documented justification, scope, duration, risk, and compensating controls. Exceptions shall not waive mandatory CJIS requirements. Any exception affecting CJI or a system used to process, store, or transmit CJI shall be coordinated with the TAC and LASO and submitted for CSO approval when required by the CJIS compensating-control process.

11. Audit Evidence

- Backup job schedules, success and failure reports, and notification records
- Daily automated integrity-verification results and business-morning review records
- Encryption, immutability, retention, multi-factor authentication, and access-control configuration evidence
- Local and offsite repository configuration and availability records
- Alternate-storage and alternate-processing designations, agreements, equipment or delivery provisions, accessibility analysis, equivalent-control validation, and priority-of-service records
- Primary and alternate telecommunications agreements, priority-of-service provisions, carrier or path single-point-of-failure analysis, and activation-test evidence
- Monthly full virtual-machine restore test plans, results, screenshots or logs, elapsed time, and corrective actions
- Annual contingency exercise plans, attendance, results, lessons learned, and corrective-action closure evidence
- Critical-system inventory, business impact analysis, service priorities, RPOs, RTOs, dependencies, and alternate-processing documentation
- Microsoft 365 nightly backup, immutable snapshot, one-year retention, restore, and annual local-only risk-review records
- Weekly Enterprise Fortress Gateway configuration-backup evidence and spare-gateway recovery records
- Recovery event records, system-owner acceptance, transaction reconciliation, actual RPO/RTO results, and reconstitution documentation

12. References

- FBI Criminal Justice Information Services (CJIS) Security Policy Version 6.0
- National Institute of Standards and Technology (NIST) NIST SP 800-53 Rev. 5 Contingency Planning (CP) controls
- National Institute of Standards and Technology (NIST) NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- Morgan County policies: MCIT-005 (Complete Policy, page 45); MCIT-007 (Complete Policy, page 63); MCIT-008 (Complete Policy, page 74); MCIT-010 (Complete Policy, page 93); MCIT-011 (Complete Policy, page 104); and MCIT-012 (Complete Policy, page 115)

13. Revision History

Version	Date	Author	Description
1.0	August 18, 2026	Information Technology Director	Draft MCIT rewrite; records-disposition safeguards clarified; pending approval

Appendices, Forms & Checklists

Appendix – Current Backup and Recovery Baseline

The following table documents the current implementation baseline. Equivalent products may replace named technologies when the replacement meets or exceeds this policy and the change is documented through County change-management procedures.

System or Data	Backup Frequency	Storage and Retention	Protection and Verification
Hyper-V virtual machines	At least every 4 hours locally; immutable local and offsite copies at least daily	Local Windows Server storage, local immutable NAS, and geographically separate offsite immutable NAS; at least 6 months	Encrypted; all accounts use MFA; automated daily integrity service and notifications; rotating full VM restore at least monthly
Microsoft 365 Government G3 tenant	Nightly	Local UniFi NAS immutable snapshots; 1 year	Encrypted; all accounts use MFA; recovery validation; local-only storage risk reviewed at least annually
UniFi Enterprise Fortress Gateway configuration	At least weekly	UniFi cloud configuration backup; backup EFG maintained	Encrypted account access with MFA; restore to spare gateway and validate security, network, logging, and alert functions

Appendix – Implementation Requirements

The following items shall be documented and tracked to completion before the County represents the associated controls as fully implemented:

- Designate the alternate processing location or service and document required authorizations or agreements, equipment or delivery capability, equivalent security controls, accessibility mitigations, and priority-of-service provisions.

- Establish and document alternate voice and data telecommunications service with appropriate priority-of-service provisions and reduced shared carrier, facility, path, or other single points of failure.
- Complete the annual risk decision for the current local-only Microsoft 365 backup and implement an additional offsite or independent protected copy if the approved risk analysis requires it.

Appendix – Recommended Records Retention

Maintain contingency plans, business impact analyses, critical-system inventories, backup and integrity records, restore-test evidence, exercise records, recovery-event records, risk reviews, exception approvals, and corrective-action records in accordance with approved County retention schedules, legal holds, CJIS requirements, and applicable law. The underlying backup data shall follow the six-month virtual-machine and one-year Microsoft 365 retention baselines established by this policy unless a longer requirement applies.

Upon expiration of the applicable retention period, and after confirming that no legal hold, audit, litigation matter, public-records request, or other preservation requirement applies, records shall be securely destroyed in accordance with MCIT-005 Media Protection Policy (Complete Policy, page 47). Destruction shall be documented where required.

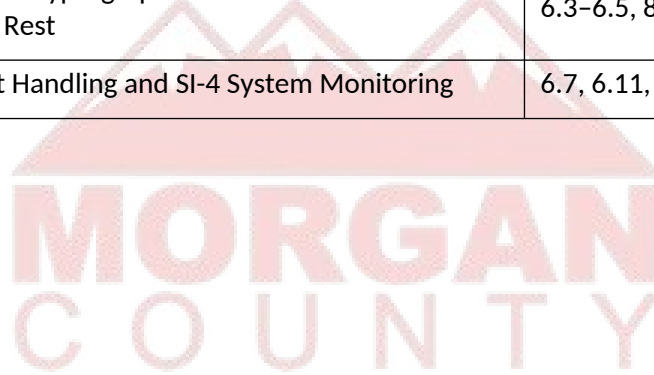
Appendix – Policy Maintenance

This policy and its procedures shall be reviewed at least annually and following contingency tests or exercises, failed restore tests, assessment or audit findings, significant system or operating-environment changes, or security incidents or breaches involving unauthorized access to CJJ or systems used to process, store, or transmit CJJ. Significant revisions require approval by the Morgan County Commission.

Appendix – CJIS & NIST Control Mapping

Control	Policy Section
CJIS/NIST CP-1 Policy and Procedures	Sections 1–13; Policy Maintenance
CJIS/NIST CP-2(1)(3)(8) Contingency Plan, Coordination, Resumption, and Critical Assets	6.1–6.2, 6.6, 6.10–6.14, 7, 8.4–8.5
CJIS/NIST CP-3 Contingency Training	6.9, 7.3–7.5, 8.5
CJIS/NIST CP-4(1) Contingency Plan Testing and Coordination	6.8–6.9, 8.3, 8.5, 8.8

Control	Policy Section
CJIS/NIST CP-6(1)(3) Alternate Storage Site, Separation, and Accessibility	6.3, 6.6–6.8, 8.1–8.4
CJIS/NIST CP-7(1)(2)(3) Alternate Processing Site	6.1–6.2, 6.6, 8.4–8.5; Implementation Requirements
CJIS/NIST CP-8(1)(2) Telecommunications Services	6.2, 6.10, 8.5, 8.7; Implementation Requirements
CJIS/NIST CP-9(1)(8) System Backup, Reliability/Integrity Testing, and Cryptographic Protection	6.3–6.8, 6.13, 8.1–8.3, 9
CJIS/NIST CP-10(2) System Recovery, Reconstitution, and Transaction Recovery	6.1, 6.11–6.12, 8.4, 8.6–8.8
NIST IA-2 / IA-5 Multi-Factor Authentication and Authenticator Management	6.5, 8.1, 9
NIST SC-13 / SC-28 Cryptographic Protection and Protection of Information at Rest	6.3–6.5, 8.1, 9
NIST IR-4 Incident Handling and SI-4 System Monitoring	6.7, 6.11, 8.2, 8.4, 8.8



Policy Library Appendix

Consolidated Definitions

This appendix consolidates key terms used throughout MCIT-001 through MCIT-015. The definitions are concise operational definitions for Morgan County. They support consistent interpretation but do not replace a more specific definition or requirement in governing law, regulation, contract, the FBI CJIS Security Policy, a NIST publication, or an individual County policy.

Coverage: 82 terms **Library:** MCIT-001 through MCIT-015 **Compiled:** August 4, 2026

A

Acceptable Use

Use of County information technology resources in a lawful, authorized, ethical, and secure manner that supports County business and complies with County policy.

Source policy: MCIT-001; MCIT-013

Access Authorization

Documented approval that permits a person, account, process, or device to access specified information or resources for an approved business purpose.

Source policy: MCIT-002; MCIT-003

Access Control

Administrative, physical, and technical measures used to grant or deny access to information, systems, services, or facilities according to approved rules.

Source policy: MCIT-003

Antivirus

Software or a managed security service that detects, blocks, quarantines, and helps remove malicious software from an endpoint or server.

Source policy: MCIT-007; MCIT-014

Audit Log

A chronological record generated by a system or application that documents events, user activity, security activity, and administrative actions.

Source policy: MCIT-011

Audit Record

An individual record or collection of records retained as evidence of an event, transaction, access, configuration change, or security-relevant action.

Source policy: MCIT-011

Authentication

The process of verifying the identity of a user, process, or device before access is allowed.

Source policy: MCIT-009

B

Backup Media

Electronic storage used to retain backup copies of information or systems for recovery, continuity, or archival purposes.

Source policy: MCIT-005; MCIT-015

Badge

A physical or electronic credential used to identify an individual and, when authorized, permit entry to a controlled or secure area.

Source policy: MCIT-006

Baseline Configuration

The documented, reviewed, and approved set of system settings, software, firmware, and security controls used as the standard for deployment and change evaluation.

Source policy: MCIT-010

C

Chain of Custody

A documented record of possession, handling, transfer, storage, and disposition that preserves the integrity and accountability of evidence, records, or media.

Source policy: MCIT-005; MCIT-011

Change Request

A documented proposal to add, remove, or modify a configuration item, including the business reason, risk, testing, approval, implementation, and rollback information appropriate to the change.

Source policy: MCIT-010

Configuration Drift

A condition in which a system's actual configuration differs from its approved baseline because of unauthorized, undocumented, or unintended changes.

Source policy: MCIT-010

Configuration Item (CI)

A hardware, software, firmware, service, network, documentation, or other managed component whose configuration is controlled and tracked.

Source policy: MCIT-010

Contingency Plan

Documented roles, priorities, resources, communications, and procedures used to sustain or restore essential services after a disruption.

Source policy: MCIT-015

Controlled Area

A location where physical entry is limited, managed, or monitored to protect County personnel, systems, equipment, records, or information.

Source policy: MCIT-006

County-Owned Device

A computer, server, mobile device, or other technology asset purchased, leased, or otherwise controlled by Morgan County.

Source policy: MCIT-013; MCIT-014

Credential

Information or an object used to establish identity or authority, such as a password, passkey, certificate, hardware token, badge, or biometric authenticator.

Source policy: MCIT-009

Criminal Justice Information (CJI)

FBI CJIS-provided data needed by law enforcement or civil agencies to perform authorized missions, including biometric, identity-history, biographic, property, and case or incident-history data.

Source policy: Library-wide; MCIT-001; MCIT-002

D

Data Custodian

The person or organizational function responsible for operating and maintaining safeguards, storage, access mechanisms, backups, and other controls for information on behalf of the data owner.

Source policy: MCIT-004

Data Owner

The official or business function accountable for determining information classification, authorized use, access requirements, retention, and protection needs.

Source policy: MCIT-004

Destruction

The physical or logical process of making media or information permanently unusable and unrecoverable when reuse is not intended.

Source policy: MCIT-005

Disclosure

The release, communication, display, transmission, or other provision of information to another person, organization, system, or destination.

Source policy: MCIT-004

E

Emergency Change

A change that must be implemented outside the normal schedule to restore service, address an urgent operational condition, or reduce a significant security risk, with expedited approval and retrospective documentation.

Source policy: MCIT-010

Endpoint Detection and Response (EDR)

Technology that continuously monitors endpoints, detects suspicious or malicious activity, supports investigation, and enables containment or remediation actions.

Source policy: MCIT-007

Escort

An authorized person who continuously accompanies and monitors a visitor or other individual requiring supervised access to a controlled area.

Source policy: MCIT-006

I

Identity Provider

A system or service that establishes and manages digital identities and provides authentication information to applications or other relying systems.

Source policy: MCIT-009

Immutable Backup

A backup copy protected from alteration or deletion for a defined retention period.

Source policy: MCIT-015

Impact

The magnitude of harm that could result from a threat event, including effects on County operations, assets, individuals, legal obligations, finances, or reputation.

Source policy: MCIT-012

Incident

An event that threatens the confidentiality, integrity, or availability of County systems or information, including unauthorized access or modification, malware, equipment theft or damage, denial-of-service activity, resource misuse, or significant IDS/IPS alerts.

Source policy: MCIT-008

Incident Severity Levels (S1-S4)

Morgan County classifies incidents as S1 Critical (major data breach or widespread outage; one-hour response target), S2 High (targeted malware or system compromise; four-hour response target), S3 Medium (unauthorized-access attempts; one-business-day response target), or S4 Low (non-malicious anomalies; logged for review).

Source policy: MCIT-008

Indicator of Compromise (IOC)

Observable evidence that may indicate a system, account, network, or data set has been attacked or compromised.

Source policy: MCIT-007

Integrity

The property that information and systems have not been improperly altered or destroyed and remain accurate, complete, and trustworthy.

Source policy: MCIT-007

L

Least Privilege

The principle of granting each user, process, or device only the minimum access and resources required to perform assigned duties.

Source policy: MCIT-002; MCIT-003

Likelihood

The assessed probability that a threat event will occur and successfully exploit a vulnerability under existing conditions and controls.

Source policy: MCIT-012

Logical Access

The ability to use or interact with systems, applications, services, accounts, or information through electronic means.

Source policy: MCIT-003

M

Malware

Software or code intended to disrupt operations, damage systems, evade controls, obtain unauthorized access, or compromise information.

Source policy: MCIT-007

Media

Physical or electronic material capable of storing, processing, or conveying information, including paper, drives, disks, tapes, memory devices, and other storage technologies.

Source policy: MCIT-005

Minimum Necessary

Limiting access, use, or disclosure of information to the smallest amount reasonably required to perform an authorized task.

Source policy: MCIT-004

Mobile Device Management (MDM)

A centrally administered service used to enroll, configure, secure, monitor, and, when authorized, lock or wipe mobile devices.

Source policy: MCIT-014

Multi-Factor Authentication (MFA)

Authentication that requires two or more distinct factor types, such as something known, something possessed, or a biometric characteristic.

Source policy: MCIT-009

N

Need-to-Know

A determination that access to specific information is necessary for an individual to perform an authorized duty, even when the individual otherwise has an appropriate role or clearance.

Source policy: MCIT-003

P

Personally Identifiable Information (PII)

Information that can distinguish or trace an individual's identity, alone or when combined with other information linked or linkable to that individual.

Source policy: MCIT-004

Personnel Security

Administrative and operational safeguards used to evaluate suitability, define responsibilities, manage access, and address personnel changes throughout the employment or service lifecycle.

Source policy: MCIT-002

Phishing

A social-engineering technique that uses deceptive messages, websites, calls, or other communications to induce a person to disclose information, transfer value, or perform an unsafe action.

Source policy: MCIT-001

Physical Access

The physical ability, right, or privilege to enter a location or to view, modify, or use systems, equipment, records, or CJI by physical presence.

Source policy: MCIT-003; MCIT-006

Physical Access Device

A key, card, badge, token, biometric reader, lock, or other mechanism used to grant, restrict, or record physical entry.

Source policy: MCIT-006

Portable Computing Device

A County-authorized laptop, tablet, mobile device, or similar equipment designed to be transported and used away from a fixed workstation.

Source policy: MCIT-014

Privileged Account

An account authorized to perform security-relevant or administrative functions beyond those available to a standard user account.

Source policy: MCIT-002; MCIT-003; MCIT-009

Privileged Activity

Use of elevated permissions to administer, configure, secure, inspect, or otherwise control systems, accounts, applications, or data.

Source policy: MCIT-011

R

Reconstitution

Returning a recovered system to a fully operational, secured, validated, and monitored known state after temporary recovery activities are complete.

Source policy: MCIT-015

Recovery Point Objective (RPO)

The maximum approved period of data loss measured backward from a disruption. Morgan County's formal RPO is 24 hours unless a system-specific plan establishes a shorter value.

Source policy: MCIT-015

Recovery Time Objective (RTO)

The maximum approved time to restore an essential service after a disruption. Morgan County's formal RTO is 24 hours unless a system-specific plan establishes a shorter value.

Source policy: MCIT-015

Remote Access

Access to County systems or information from outside the local County-controlled network or facility boundary through an approved connection and security controls.

Source policy: MCIT-003; MCIT-014

Remote Work

Authorized performance of County duties from a location outside the employee's normal County worksite using approved practices, devices, and connections.

Source policy: MCIT-014

Removable Media

Portable media that can be inserted into and removed from a computing device, including USB storage, memory cards, removable drives, optical media, and similar devices.

Source policy: MCIT-005

Residual Risk

Risk remaining after safeguards and other risk responses have been implemented.

Source policy: MCIT-012

Restore Test

A controlled recovery of backup information used to verify that data can be retrieved, decrypted, mounted, started, and validated.

Source policy: MCIT-015

Risk

The potential adverse effect of a threat exploiting a vulnerability, considered in terms of likelihood and impact.

Source policy: MCIT-012

Risk Acceptance

A documented management decision to acknowledge and retain a risk within approved authority and tolerance rather than further avoid, mitigate, or transfer it.

Source policy: MCIT-012

Risk Owner

The official or organizational role accountable for monitoring a risk and ensuring that an approved response is selected, implemented, and reviewed.

Source policy: MCIT-012

Role-Based Access Control (RBAC)

An access-control approach in which permissions are assigned to defined job or functional roles and users receive access through approved role membership.

Source policy: MCIT-003

Role-Based Training

Security or privacy training tailored to the responsibilities, access, systems, and risks associated with a person's assigned role.

Source policy: MCIT-001

Rollback Plan

Documented steps for reversing a change and restoring the prior approved state if implementation fails or causes unacceptable effects.

Source policy: MCIT-010

S

Sanitization

A process that renders access to target data on media infeasible for a given level of effort while allowing the media to be reused or disposed of as authorized.

Source policy: MCIT-005

Secure Area

A physical location protected by access restrictions and other safeguards appropriate to the systems, equipment, records, or information located there.

Source policy: MCIT-006

Security Awareness

Knowledge and attention that help personnel recognize security responsibilities, identify threats, and take appropriate protective or reporting actions.

Source policy: MCIT-001

Security Event

An observable occurrence in a system or network that may be relevant to security, policy compliance, operations, or an investigation; an event is not necessarily an incident.

Source policy: MCIT-011

Security Information and Event Management (SIEM)

Technology that collects, retains, correlates, searches, and analyzes security logs and events to support monitoring, detection, investigation, and reporting.

Source policy: MCIT-011

Security Patch

A vendor or developer update intended to correct a security weakness, vulnerability, or defect in software or firmware.

Source policy: MCIT-007

Sensitive PII

PII that, if lost, compromised, or disclosed without authorization, could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual or create significant risk to the County.

Source policy: MCIT-004

Separation

The end of an employment, contract, volunteer, or other service relationship, including the process for promptly removing access and recovering County property.

Source policy: MCIT-002

Service Account

A non-person account used by an application, system, device, or automated process to perform defined functions.

Source policy: MCIT-009

Shared Account

An account used by more than one person. Shared accounts reduce individual accountability and are allowed only when specifically authorized and controlled.

Source policy: MCIT-009

Social Engineering

Manipulation of people through deception, impersonation, urgency, or other influence techniques to obtain information, access, money, or an unsafe action.

Source policy: MCIT-001

System Owner

The official or organizational function accountable for a system's business purpose, operational requirements, access decisions, risk, and lifecycle oversight.

Source policy: MCIT-010

T

Threat

A circumstance or event with the potential to adversely affect County operations, assets, individuals, or information through unauthorized access, destruction, disclosure, modification, or denial of service.

Source policy: MCIT-012

Time Synchronization

The process of maintaining consistent, authoritative time across systems so audit records and security events can be accurately correlated.

Source policy: MCIT-011

U

Unauthorized Change

A modification to hardware, software, firmware, configuration, data, or documentation that was not properly requested, approved, implemented, or recorded.

Source policy: MCIT-007; MCIT-010

V

Virtual Private Network (VPN)

An approved encrypted connection that protects communications and provides controlled remote access across an untrusted network.

Source policy: MCIT-014

Visitor

A person who is not assigned routine authorized access to an area and who must follow visitor identification, logging, escort, or monitoring requirements.

Source policy: MCIT-006

Vulnerability

A weakness in a system, process, configuration, safeguard, or environment that could be exploited or triggered by a threat.

Source policy: MCIT-007; MCIT-012

Reference Sources

These sources informed the terminology and should be consulted when an authoritative or control-specific definition is required.

- Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy Version 6.0*, December 27, 2024. [Official PDF](#)
- National Institute of Standards and Technology, *Computer Security Resource Center Glossary*. [Official glossary](#)
- NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.
- NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*.
- NIST Special Publication 800-88 Revision 2, *Guidelines for Media Sanitization*.

Library maintenance note: Review this appendix whenever a policy is added, materially revised, or updated to use a new defined term.





Limit of 3 Minutes

- *Please do not repeat previously stated comments**
- *The Commission cannot respond –
This is not a Q & A**
- *Please Be Respectful**

Thank you for being here!

August 14th, 2026



EAGLE VISTA

MORGAN COUNTY

Prepared by:



MOUNTAIN GREEN UTAH



EAGLE VISTA

MORGAN COUNTY



Community Summary:

Eagle Vista is a thoughtfully designed 44-acre master-planned community in Mountain Green, Utah, that blends quality housing, neighborhood commercial, open space, and recreational amenities into a connected and walkable neighborhood. Featuring 270 homes with single-family residences alongside some luxury townhomes, as well as 2.5 acres of commercial space to serve residents and the surrounding area. The community provides multiple, diverse housing opportunities for those looking for a place to call home.

The community is organized around a network of interconnected streets, landscaped open space, sidewalks, trails, sports courts, and gathering spaces that encourage walkability and neighborhood interaction. Ten acres of the project - nearly a quarter of the site - is dedicated to open space, including preserved natural areas along the creek corridor, landscaped common areas, public play spaces and trail connections that allow residents to enjoy the natural beauty of Mountain Green.

At the heart of Eagle Vista is a clubhouse and recreation area featuring a fitness center, community gathering space, public pickleball courts, and outdoor amenities designed to support an active lifestyle and foster a strong sense of community. The development also includes public trailhead access, connectivity to surrounding neighborhoods, and open-space amenities that provide lasting benefits for both residents and the broader Mountain Green community.

With its combination of a variety of housing types, neighborhood-serving commercial space, thoughtfully planned open space, high-quality architecture, and recreational opportunities, Eagle Vista represents an approach to growth that complements the character of Mountain Green and preserves the value of the community and property values.



Table of Contents

Introduction:	4
Applicant & Landowner Contact Information	4
Legal Description & Survey	5
Adjacent Land Ownership & Use	6
Community Master Plan	7
Area Use & Unit Tables	7
Subdivision Character	8
Phasing Map	11
Transportation Plan	12
Street Cross Sections	13
Transportation Guidelines	14
Technical Information	14
Utilities	14
Community Design Guidelines:	15
Architectural Design Standards	15
Setbacks & Height Regulations	29
Infrastructure Design & Maintenance	30
Lighting Design	30
Open Space	31
10 AC	31
Open Space Standards	32
Open Space Example Images	33
Community Renderings (Previous rendition)	34

Introduction:

Applicant & Landowner Contact Information

Property Owner Name: BCP Development LLC

Address: 300 S 1350 E, Floor 2, Lehi, UT 84043

Phone Number: 801-766-4442

Email Address: Luke@flagshiphomes.com

INTRODUCTION

The Eagle Vista community is located in Mountain Green, a community in Morgan County. To the south of the property is interstate 84 and to the north of the development is Old Highway Road.



Legal Description & Survey



LEGAL DESCRIPTION(S) (FROM TITLE REPORT)

Parcel 1:

A part of the North half of the Southeast quarter and the Southwest quarter of the Northeast quarter of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian

Beginning at a point which bears South 00°06' East 2504.4 feet from the North quarter Section Corner Stone of the said Section 25, and running thence along the Southerly side of the State Road, U.S. 30-S; South 47°17' East 226.0 feet to a point on the South bank of cottonwood creek; thence along said bank South 76°00' West 176.1 feet; thence South 161.3 feet; thence South 75°40' East 160.0 feet; thence North 25°50' East to the State Road; thence along said road South 47°17' East 22.0 feet; thence along the arc of a 05°45' curve to the left 406.66 feet (the radius of said curve is 995.4 feet and the tangent is 206.13 feet and the central angle is 23°23'); thence South 70°40' East 1639.7 feet; thence along a 04°07' curve to the right 613.0 feet to the Range Line; (data for full curve; central angle 26°37' Right; Degree 04°07' Radius 1392.7 feet; Tangent 329.43 feet; curve length 646.56 feet); thence South on said Range Line 154.3 feet to the 40 acre corner; (said 40 acre corner bears South 1347.0 feet from the East quarter corner of the said Section 25); thence South 89°57' West 1330.78 feet to the 40 acre corner; thence 5 courses along the meadow about one rod distant Southerly from the foot of the slope of the bench as follows; North 63°40' West 613.0 feet; thence North 47°46' West 231.8 feet; thence North 82°00' West 225.0 feet; thence South 59°00' West 172.5 feet; thence South 69°02' West 256.58 feet to the quarter Section line; thence along said line North 00°06' West 330.0 feet; thence West 1330.73 feet to the 40 acre line; thence along said line North 00°08' West 720.05 feet to the quarter section line; thence along said line North 89°42' East 1331.16 feet to the quarter section line; thence along said line North 00°06' West 127.6 feet to the point of beginning.

Less the following description of real property which has been sold and conveyed to the Board of Education, Morgan County School District. A part of the Southeast 1/4 of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian U.S. Survey: Beginning at the Southeast corner of the Northeast 1/4 of said Southeast 1/4 Section; said point is South 1347.0 feet from the East 1/4 corner of said Section 25, running thence South 89°57' West 1330.78 feet along the 40 acre line to the 40 acre corner; thence North 63°40' West 158.00 feet; thence North 30°27' East 714.15 feet to the South line of the State Road U.S. 30-S; thence 2 courses along said South line as follows: South 70°40' East 630.00 feet and Easterly along the arc of a 1392.7 foot radius curve to the right 613.00 feet to the Section line; thence South 154.30 feet along the Section line to point of beginning.

Less and excepting therefrom those portions conveyed in that certain Warranty Deed, recorded February 20, 2001 as Entry No. 84249, in Book 165 at Page 841, of the Official Records and being described as follows:

A tract of land situated in the Southeast Quarter of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian, U.S. Survey, Morgan County, Utah:

Commencing at the East Quarter Corner of said Section 25, a rebar and cap; thence South 89°30'37" West 2,427.67 feet along the Quarter Section line; thence South 00°00'00" East 85.06 feet to a point on the South line of Old Highway Road and the Northeast Corner of the J. Todd Vogt property as recorded in the Morgan County Recorder's Office in Book M127 at Page 507 and the true point of beginning; thence South 47°17'00" East 22.00 feet along said South line of Old Highway Road; thence Southeasterly 213.72 feet along said South line of Old Highway Road, a tangent curve to the left having a radius of 995.40 feet, an included angle of 12°18'07" and a long chord bearing South 53°26'04" East 213.31 feet; thence South 35°47'54" West 159.32 feet; thence North 62°44'49" West 203.12 feet to the Southeast corner

of the Vogt parcel; thence North 25°50'00" East 198.00 feet along the East line of said Vogt parcel to the point of beginning.

Less and excepting therefrom those portions conveyed in that certain Quit Claim Deed, recorded June 28, 2001 as Entry No. 85491, in Book 171 at Page 123, of the Official Records and being described as follows:

A tract of land situated in the Southeast Quarter of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian, U.S. Survey, Morgan County, Utah.

Commencing at the East Quarter Corner of said Section 25, a rebar and cap; thence South 89°30'37" West 2427.67 feet along the Quarter Section line; thence South 00°00'00" East 85.06 feet to a point on the South line of Old Highway Road and the Northeast corner of the J. Todd Vogt property as recorded in the Morgan County Recorder's Office M127-507; thence South 25°50'00" West 198.00 feet along the Easterly line of said property to the Southeast Corner of said Vogt property, the true point of beginning; thence South 62°44'49" East 203.12 feet; thence South 35°47'54" West 29.30 feet; thence North 62°44'49" West 198.05 feet; thence North 25°50'00" East 28.98 feet to the Southeast Corner of the J. Todd Vogt property and the point of beginning.

The basis of bearing is the North line of the Southeast Quarter of said Section 25 called: South 89°30'37" West as monumented.

Parcel 2:

A tract of land situated in the Southeast Quarter of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian, U.S. Survey, Morgan County, Utah.

Commencing at the East Quarter Corner of said Section 25, a rebar and cap; thence South 89°30'37" West 2427.67 feet along the Quarter Section line; thence South 00°00'00" East 85.06 feet to a point on the South line of Old Highway Road and the Northeast corner of the J. Todd Vogt property as recorded in the Morgan County Recorder's Office M127-507; thence South 25°50'00" West 198.00 feet along the Easterly line of said property to the Southeast corner of said Vogt Property, the true point of beginning; thence South 62°44'49" East 203.12 feet; thence South 35°47'54" West 29.30 feet; thence North 62°44'49" West 198.05 feet; thence North 25°50'00" East 28.98 feet to the Southeast corner of the J. Todd Vogt property and the point of beginning.

The basis of bearing is the North line of the Southeast quarter of said Section 25 called: South 89°30'37" West as monumented.

Parcel 3:

Part of the Northwest Quarter of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian.

Beginning at a point located East 1167.8 feet and North 430.3 feet and South 85°25' West 136.0 feet and South 63°45' West 87.6 feet from the West Quarter corner of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian, running thence North 528.06 feet to the South right of way line of the State Road, thence North 85°50'00" East 35.00 feet along said South right of way line, thence South 69.00 feet, thence South 5°40'28" West 80.00 feet, thence South 343.00 feet, thence south 22°37'20" east 23.08 feet, thence 63°45'00" west 40.00 feet to the point of beginning.

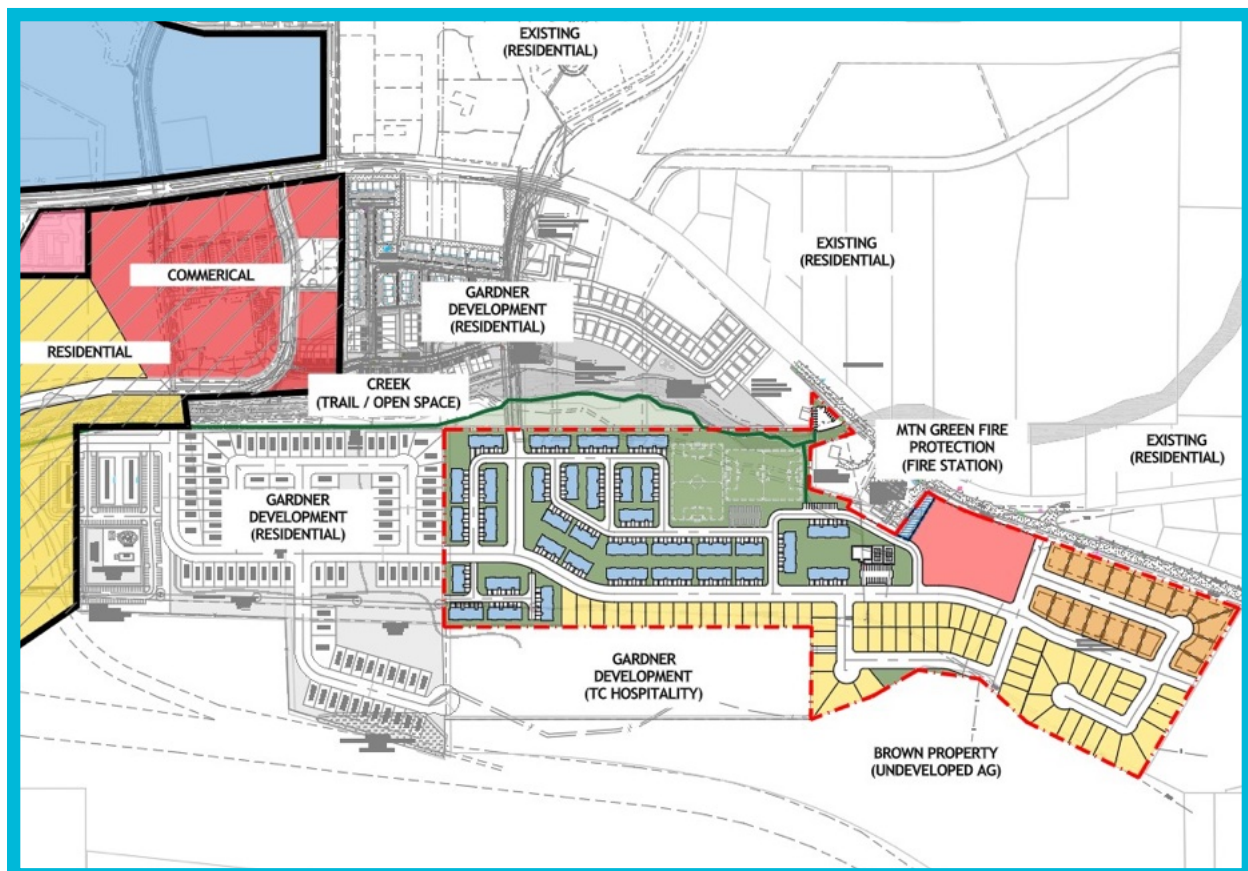
Together with Parcels 1-3 an easement for ingress and egress as set for forth in that Quit Claim Deed Easement Estate recorded May 23, 2023, as Entry No. 163503, in Book 400 at Page 503, of the Official Records.

NOTE: BEARINGS AND DISTANCES FROM TITLE REPORT DOES NOT CLOSE.

Adjacent Land Ownership & Use

Adjacent Land Ownership & Use Map Explanation

Adjacent land ownership is illustrated in the accompanying map exhibit. Major surrounding landowners include Gardner Group residential development to the west, north west and south west of site; Bonnie Brown to the south east of site which currently used as agriculture with Rural Residential planned used; Mountain Green Fire Protection District to the north east of site alongside existing residential across Old Highway Road.

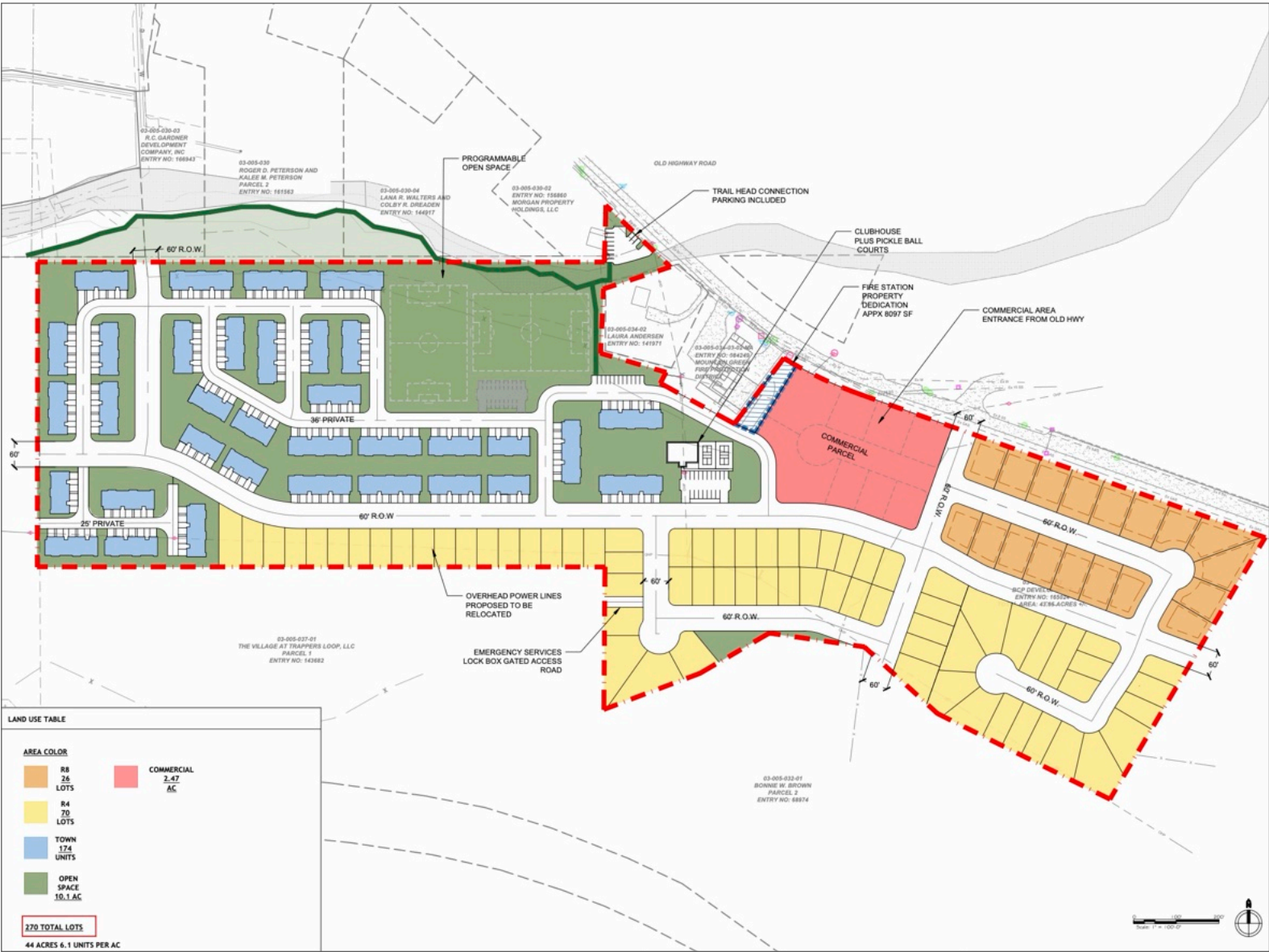


Community Master Plan

Area Use & Unit Tables

TOWN CENTER ZONE OVERLAY

Total Acreage: **44 Acres**
Total Phases: **3 Phases**
Unit Count: **270 Units**
Zones: **Town Center Zone (Morgan County § 155.265) + R1-8**



Subdivision Character

Overview

The proposed Mountain Green subdivision is designed to meet Morgan County's Town Center zoning requirements while creating a neighborhood that is welcoming, walkable, and built to last. The project integrates three complementary housing types — townhomes, small single-family detached homes, and traditional single-family homes on 8,000-square-foot lots — to serve a broad range of residents, from first-time buyers and young families to long-term homeowners and retirees.

The development emphasizes pedestrian-friendly design, preserved green space, and sustainable building practices — all consistent with the county's vision for the Mountain Green community.

Housing Options and Community Design

By offering three distinct housing types within a single, cohesive neighborhood, the subdivision creates genuine variety without sacrificing visual harmony or community character.

Townhomes provide an attainable entry point into homeownership for individuals, couples, and small families. Shared maintenance reduces the burden on individual owners, and the close-knit layout naturally encourages neighborly interaction and a strong sense of community.

Small single-family detached homes offer the privacy of a standalone home with a more modest footprint — appealing to young professionals, empty nesters, and anyone seeking low-maintenance living without sacrificing independence. Smaller lots also preserve more land for green space and open areas throughout the neighborhood.

Traditional single-family homes on 8,000-square-foot lots deliver the space and stability that families and long-term residents value most. These homes allow for outdoor living, gardening, and family gatherings, and their varied architectural styles contribute to the visual interest and identity of the neighborhood.

Across all three housing types, the subdivision is designed with walkability in mind. Pedestrian pathways connect homes to parks, open spaces, and nearby amenities, reducing vehicle dependence and encouraging residents to engage with their surroundings.

Public Benefits

This project delivers a meaningful set of public benefits to Mountain Green and the surrounding community:

- **Fire Station Land Donation.** The developer is donating 8,097 square feet of property to the neighboring fire station. This contribution directly supports the station's operational capacity and ensures that emergency services remain effective and accessible for all residents in the area.
- **Trail Access Along Cottonwood Creek.** The subdivision will provide public access to a trail corridor along Cottonwood Creek, giving residents and neighbors a valued recreational amenity that connects people to the natural landscape and supports an active outdoor lifestyle.
- **Recreational Amenities.** Large community park and pickleball courts will be available to both residents and the broader community, with one court designated as private and one open to the public, offering well-maintained recreational opportunities that enhance quality of life for all ages. Playground amenities to remain private and maintained by the HOA.
- **Diverse Housing Supply.** The range of housing types addresses a demonstrated local need, allowing Mountain Green to better serve households of varying sizes, life stages, and economic circumstances.
- **Underground Utility Lines.** The development will fund the under-grounding and removal of existing overhead power lines in the area. This improves the visual character of the neighborhood, increases public safety, and provides more reliable utility service for both new and existing residents.

Neighborhood Commercial: The Right-Sized Addition for this Area

Eagle Vista includes 2.5 acres of neighborhood commercial space, positioned to serve both the residents of the community and the broader Mountain Green area. This commercial component reflects careful planning of the site, its market context, and the commercial needs of the surrounding area — resulting in a commercial allocation that is scaled to be successful.

The commercial area is intended to accommodate the kinds of neighborhood-serving uses that enhance daily life — such as a café or coffee shop, small-scale retail, personal services, or professional offices — within comfortable walking distance of every home in the community. Rather than requiring residents to drive, Eagle Vista's design places these opportunities at the neighborhood's doorstep, reinforcing the walkable, connected character that defines the entire community plan.

Equally important, the commercial component is sized to thrive. Market studies show that commercial space succeeds when it is scaled to the consumer base available to support it. A 2.5-acre neighborhood commercial area, supported by the 270 households within Eagle Vista and the surrounding neighborhoods, represents a commercial presence that can attract quality tenants, maintain consistent occupancy, and contribute lasting vitality to the community — a far better outcome for Mountain Green than a larger allocation of commercial ground that the local market cannot yet absorb. Larger-format commercial development is appropriately concentrated in nearby developments to the north and west, where it will bring benefit on a greater scale, visibility, and connectivity. Together, these commercial areas form a complementary system: a cohesive commercial core nearby, and a walkable neighborhood commercial node within Eagle Vista itself.

To formalize these commitments, the developer has prepared a comprehensive Master Development Agreement in collaboration with County Planning and Legal Staff. The agreement also includes a provision to prohibit short-term rentals through the community's CC&Rs.

Financial Analysis: A Balanced Land Plan That Benefits Mountain Green

The proposed land plan — combining residential development with a properly sized commercial component — delivers revenue to Morgan County on two fronts. Single-family residential development on this site generates reliable property tax revenue for the county, while the 2.5-acre commercial area adds the opportunity for sales tax revenue from neighborhood-serving businesses.

The businesses best suited to this location — cafés, coffee shops, small retail, personal services, and professional offices — generate general sales tax and, in some cases, additional local taxes on prepared food and beverages. Critically, that revenue materializes only when businesses are open and operating successfully. By scaling the commercial component to the size the local market can genuinely support, Eagle Vista maximizes the likelihood that its commercial space will be occupied, active, and revenue-producing from the outset — rather than sitting vacant while waiting for demand to catch up. Many of these business types are subject to general sales tax and, in some cases, additional local taxes on prepared food and beverages — revenue that flows to the county only when those businesses are operating successfully. Placing commercial uses at an isolated location reduces the likelihood that these businesses will open and remain open — meaning the anticipated sales tax revenue may never materialize. Siting commercial development along Old Highway and near Lee's Market, where infrastructure and consumer traffic already exist, gives those businesses the best chance of success and delivers the greatest benefit to the county.

The result is a land plan that serves the county's long-term fiscal health on both fronts: consistent property tax revenue from a thriving residential community, and sales tax potential from commercial space positioned and sized for success.

Conclusion

The Eagle Vista plan is a thoughtfully designed, community-driven project that delivers real and lasting benefits to Mountain Green — a land donation to the fire station, public trail access along Cottonwood Creek, programmable recreational open space, amenities that are open to the broader community, a diverse housing supply, and a walkable neighborhood that brings everyday services closer to home.

The commercial component reflects a balanced approach: 2.5 acres of neighborhood-serving commercial space scaled to succeed at this location, complementing the larger commercial core planned in neighboring developments. This combination of residential and right-sized commercial development serves the county's long-term interests better than any alternative configuration for this site.

Eagle Vista represents a forward-thinking, responsible approach to growth in Morgan County — one that respects the existing character of Mountain Green while helping the community grow in a way that works for everyone.

Area Use & Unit Tabulation Table

LAND USE TABLE	COMMERCIAL ALLOCATION
AREA COLOR R8 26 LOTS R4 70 LOTS TOWN 174 UNITS OPEN SPACE 10.1 AC 270 TOTAL LOTS 44 ACRES 6.1 UNITS PER	Eagle Vista provides 2.5 acres of neighborhood commercial space, with the balance of the Town Center Zone's commercial allocation requirement addressed through the exception provisions of Morgan County Code §155.266(D)(2)(a-d). This approach reflects sound land use planning with larger commercial development occurring closer to Trappers Loop Road and Old Highway Road which will help serve Mountain Green's broader commercial needs with the adjacency, scale, and frontage those uses require, while Eagle Vista's commercial component captures the neighborhood-scale opportunity where this site is genuinely positioned to support. By concentrating larger-format commercial development closer to Trappers Loop Road and Old Highway Road, rather than fragmenting it across multiple sites, produces a more cohesive and successful commercial district for Mountain Green as a whole. At the same time, Eagle Vista's 2.5-acre commercial area is located to take advantage of the site's best frontage and access, giving neighborhood-serving businesses the visibility and convenience they need to thrive. The reduced commercial allocation also enables the community benefits described throughout this plan – ten acres of open space – public trail connections along Cottonwood Creek, recreational amenities which include a public pickleball court, and a significant contribution toward public infrastructure, which includes property for a future fire station expansion. The proposed layout advances the objectives identified in § 155.266(D)(3)(a-f) by promoting a cohesive development pattern while enhancing public amenities, connectivity, open space, and public safety improvements.

TownHome: *Luxury townhome plans with open floor plan and 2 car garage, dimensions found in design guidelines of this plan*

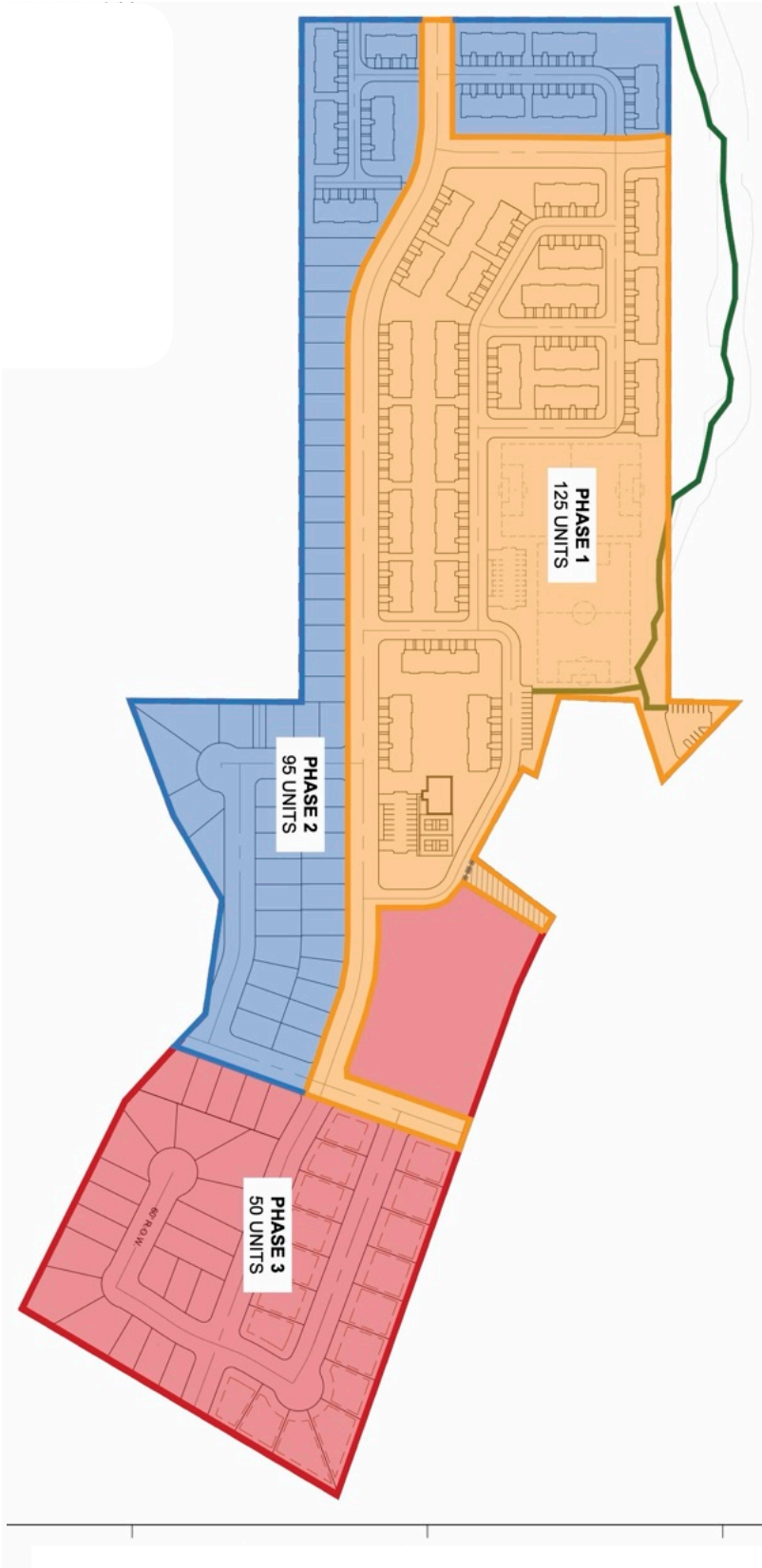
Single-Family R4 Lots: *These lots are 4000 SF lot size min (typ. lot dimension of 50' wide and 80' deep) Single-Family detached*

Single-Family R8 Lots: *These lots are 8000 SF lot size min (typ. lot dimensions area 70' wide and 100' deep) Single-Family detached*

Open Space: *10 acres of open space is provided throughout the 44-acre project site, including programmable recreation areas, landscaped common areas, and preserved natural areas along the creek corridor*

Walkable Neighborhood Commercial: *A 2.5-acre neighborhood commercial area anchors Eagle Vista with future services and gathering places within walking distance—not only for Eagle Vista residents, but for the broader Mountain Green community. This amenity does not exist in the area today; residents currently drive for even the most basic services while creating a community focal point. Intended uses are deliberately neighborhood-scaled—a café, small retail, personal services, or professional office—sited to offer walkable access from within Eagle Vista and convenient, visible frontage for the surrounding community.*

Phasing Map

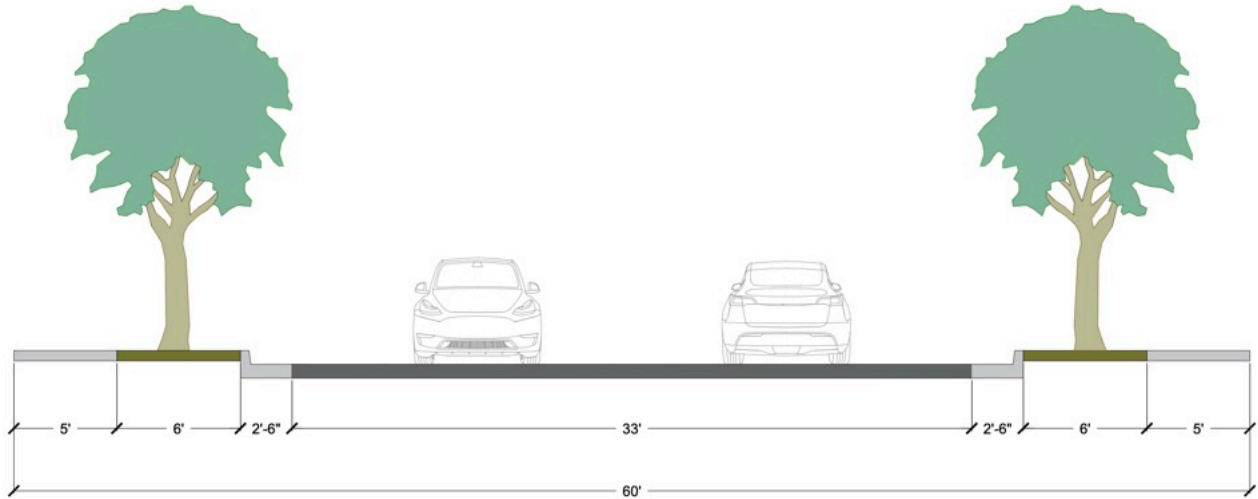


Transportation Plan

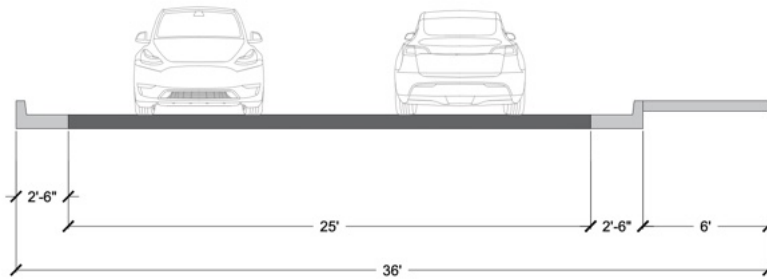


Street Cross Sections

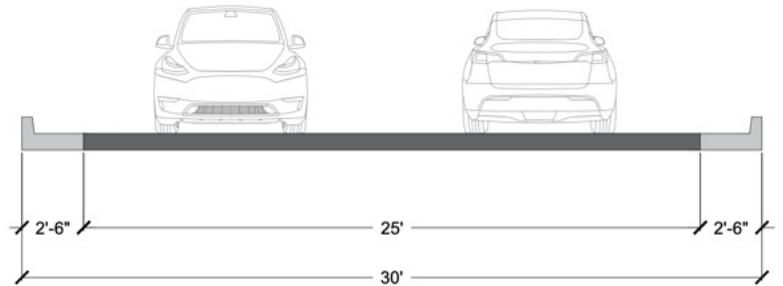
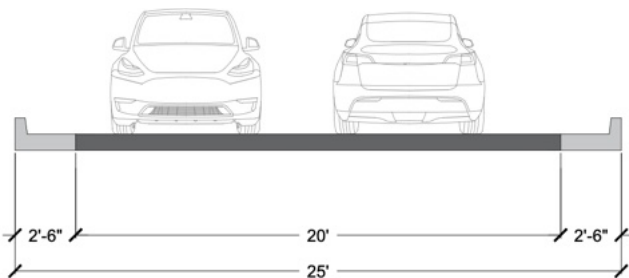
Residential Road 60' R.O.W



Private Road 36' R.O.W



Alley 25' & 30' R.O.W



Transportation Guidelines

Streets

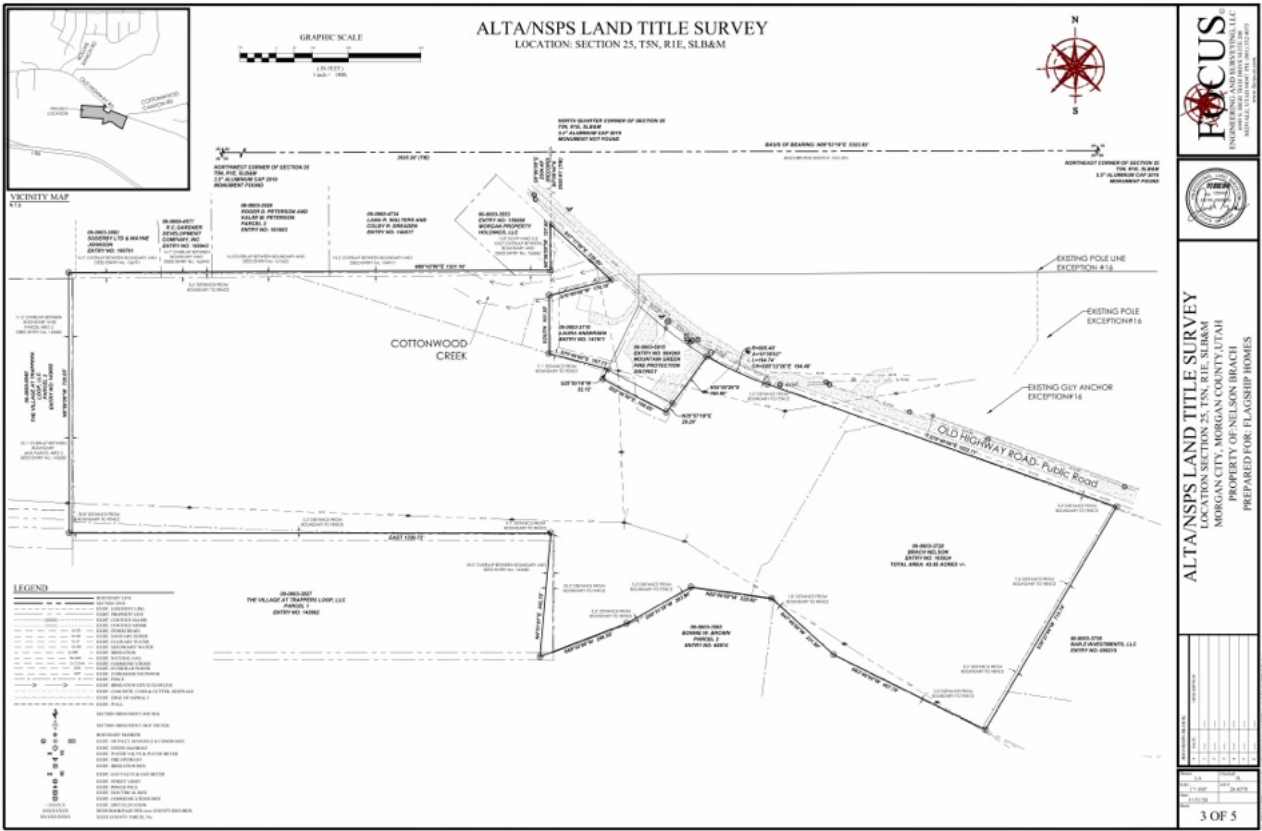
Eagle Vista is organized around a connected, hierarchical street network. The network includes, residential streets (60' R.O.W.), private streets (36' R.O.W.), and alleys (25' & 30' R.O.W.), forming a clear circulation framework. Residential Streets form the primary circulation system, creating a loop and key connections between developments. Private Streets provide internal access and emphasize low speeds and pedestrian comfort primarily for the townhome area. Alleys support loading access and reduce driveway conflicts in certain areas of the project. A connection will go from the subdivision to the Gardner Development on the west and north side of the property. Three other connections will be provided, with one connection on to Old Highway Road, and the two other connections will be to Bonnie Brown and Bar-Z investments LLC properties.

Technical Information

Geo-Technical Report by AGECE has been completed. Grading has been completed by Landmark Excavation on the site to remove the former gravel mounds from the previous owner user. Lastly the power lines are being removed offsite at the expense of the developer.

Utilities

Utilities to the site have been identified by the following providers: Cottonwood Mutual Water, Weber Basin, Mountain Green Sewer Improvement District, Enbridge Gas , Rocky Mountain Power.



ALTA Survey

Community Design Guidelines: Architectural Design Standards

R8 Area

The R8 Area will feature 5+ different plan sets that have their own distinct floor plan layout, each of those 5 consisting of 3 different elevation types (A,B and C) bringing a total of 15 different elevations on 5 unique floor plans. Furthermore there are 30+ color schematic combinations on each of those 15 elevations, bringing a grand total of 450+ unique home facade combinations to a community. Below are 5 different architectural combination examples.

Hawthorn

4 Bedroom, 2.5 Bath

Finished: 3,010 Sq.Ft., Total: 5,014 Sq.Ft



Elevation A



Elevation B



Elevation C

Olive

4 Bedroom, 2.5 Bath
Finished: 2,435 Sq.Ft.,Total: 3,935 Sq.Ft.



Elevation A



Elevation B



Elevation C

Redwood

4/5 Bedroom, 2.5 Bath
Finished: 2,380 Sq.Ft.,Total: 3,411 Sq.Ft.



Elevation A



Elevation B



Elevation C

Sequoia

4 Bedroom, 2.5 Bath
Finished: 2,248 Sq.Ft.,Total: 3,643 Sq.Ft.



Elevation A



Elevation B



Elevation C

Sycamore

5 Bedroom, 3 Bath
Finished: 2,845 Sq.Ft.,Total: 4,315 Sq.Ft.



Elevation A



Elevation B



Elevation C

R4 Area

The R4 Area will feature 5+ different plan sets that have their own distinct floor plan layout, each of those 5 consisting of 3 different elevation types (A,B and C) bringing a total of 15 different elevations on 5 unique floor plans. Furthermore there are 30+ color schematic combinations on each of those 15 elevations, bringing a grand total of 450+ unique home facade combinations to a community. Below are 5 different architectural combination examples.

Acacia

3 Bedroom, 2.5 Bath, Laundry Room Upstairs
Finished: 1,937 Sq.Ft., Total: 2,924 Sq.Ft.



Elevation A



Elevation B



Elevation C

Ash

4 Bedroom, 2.5 Bath
Finished: 2,101 Sq.Ft.,Total: 2,990 Sq.Ft.



Elevation A



Oak

4 Bedroom, 2.5 Bath
Finished: 1,977 Sq.Ft.,Total: 2,822 Sq.Ft.



Elevation A



Elevation B



Elevation C

Pine

4 Bedroom, 2.5 Bath
Finished: 2,080 Sq.Ft., Total: 3,040 Sq.Ft.



Elevation A



Elevation B



Elevation C

Spruce

4/5 Bedroom, 2.5 Bath
Finished: 2,217 Sq.Ft.,Total: 3,178 Sq.Ft.



Elevation A



Elevation B



Elevation C

Townhome Area

The Townhome Area will feature town home products. Elevations and variations of floor plan types shown below.



Type A Type B Type C Type D Type E Type F

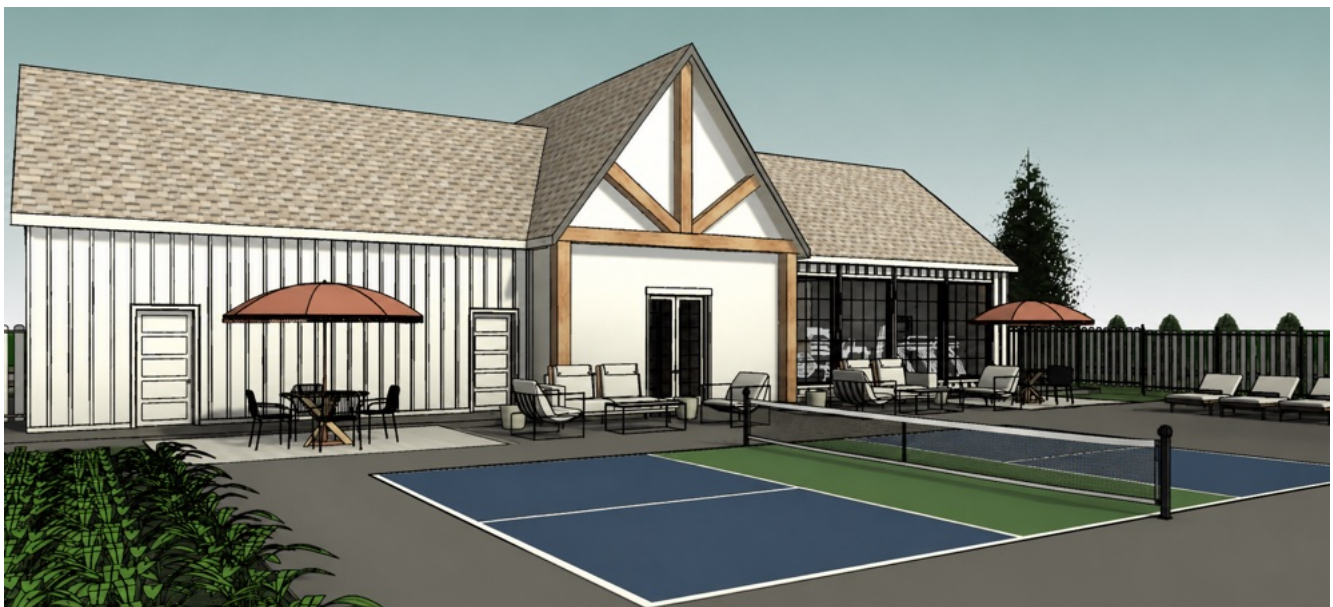


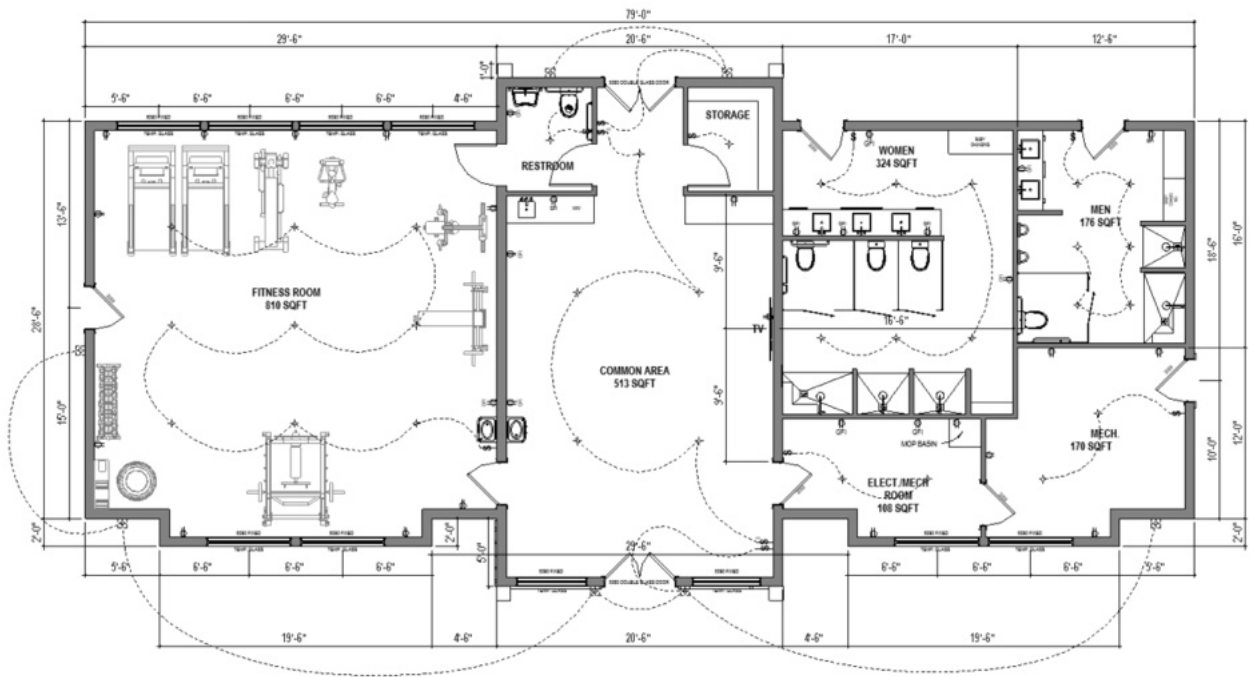


Clubhouse + Amenities

The proposed clubhouse is a resident amenity center featuring a fitness room, central gathering space, locker rooms, and pickleball support facilities. The building includes an 810-square-foot fitness center, a 513-square-foot common area for social and community activities, men's and women's locker rooms, storage, restroom facilities. The layout is designed to provide convenient access to fitness and recreational amenities while supporting resident gatherings and community events.

Architectural features may vary from what is graphically shown in final submittal





Setbacks & Height Regulations

Per § 155.134 SETBACK AND YARD REGULATIONS of Morgan County Code

Per § 155.133 HEIGHT REGULATIONS of Morgan County Code

Development Criteria			
	Multifamily (Town home area Town Center)	Single Family Town Center (4000 SF min. lots)	Single Family Dwelling R8 (8000 SF min. lots)
Building Configuration			
Principle Building	2 Stories (35 ft.)	2 Stories (35 ft.)	2 Stories (35 ft.)
Accessory Structures	1 Story Max	1 Story Max	1 Story Max
Min. Lot Size	N/A	4,000 SF	8,000 SF
Max. Building Coverage Footprint	N/A	35%	35%
Setbacks Principle Building			
Front	10 ft.	25 ft.	25 ft.
Side	5 ft.	10 ft.	10 ft.
Rear	5 ft.	20 ft.	20 ft.
Setbacks - Accessory Structure (From Principle)			
Front	N/A	5 ft.	5 ft.
Side	N/A	0 ft.	0 ft.
Rear	N/A	0 ft.	0 ft.

Infrastructure Design & Maintenance

Roads, curb & gutter and sidewalks infrastructure installed within the public right-of-way will be turned over after acceptance for maintenance and long-term care. Design elements such as street lighting, and signage are to be maintained by HOA. Ample amount of parking will be provided to accommodate visitors and guests.

Lighting Design

Public lighting should comply with Morgan county's outdoor lighting requirements as Per § 155.352. Lighting for all public and private thoroughfares within Eagle Vista should follow those standards outlined.

Open Space
10 AC



Open Space Standards

Overview

The Eagle Vista development incorporates 10 acres of open space – nearly a quarter of the 44-acre site – in a comprehensive network designed to preserve natural features, provide recreational opportunities, and enhance the overall character of the community. Open space areas are distributed throughout the site to ensure accessibility, connectivity, and long-term usability. The plan includes both natural open space and productive open space, forming an integrated system of parks, buffers, and preserved landscape areas.

Maintenance Responsibilities

HOA to maintain landscaping in park area. All other areas are HOA or as specified, park strips in local roads (60') by adjacent lot owners.

Natural Open Space

Natural open space areas are primarily located along the project perimeter areas. These spaces are intended to:

- Preserve existing natural features and drainage patterns
- Provide visual buffers between adjacent properties
- Maintain a transition between developed areas and surrounding land uses
- Support passive recreation such as walking, trails, and informal use. This is mainly on the north side of this project where the creek bed area exists.

These areas are generally maintained in a natural or minimally improved condition and may include trail connections where appropriate.

HOA Open Space

HOA open space is incorporated within and adjacent to neighborhood areas and is designed for active use and community benefit. These areas include:

- Open lawn and flexible recreational spaces
- Clubhouse Amenity
- Pickleball Courts

Productive open space is intended to provide usable outdoor areas for residents, support neighborhood identity, and distribute recreation opportunities throughout the development.

Open Space Example Images



Front yard example in Town Home



Town Home area Example w/ Garden Area



Clubhouse with Pickleball Court Example



Open Space Trail Network, Example



Large Open Space Park

Community Renderings *(Previous rendition)*



OVERALL



TOWN HOME VIEW WEST



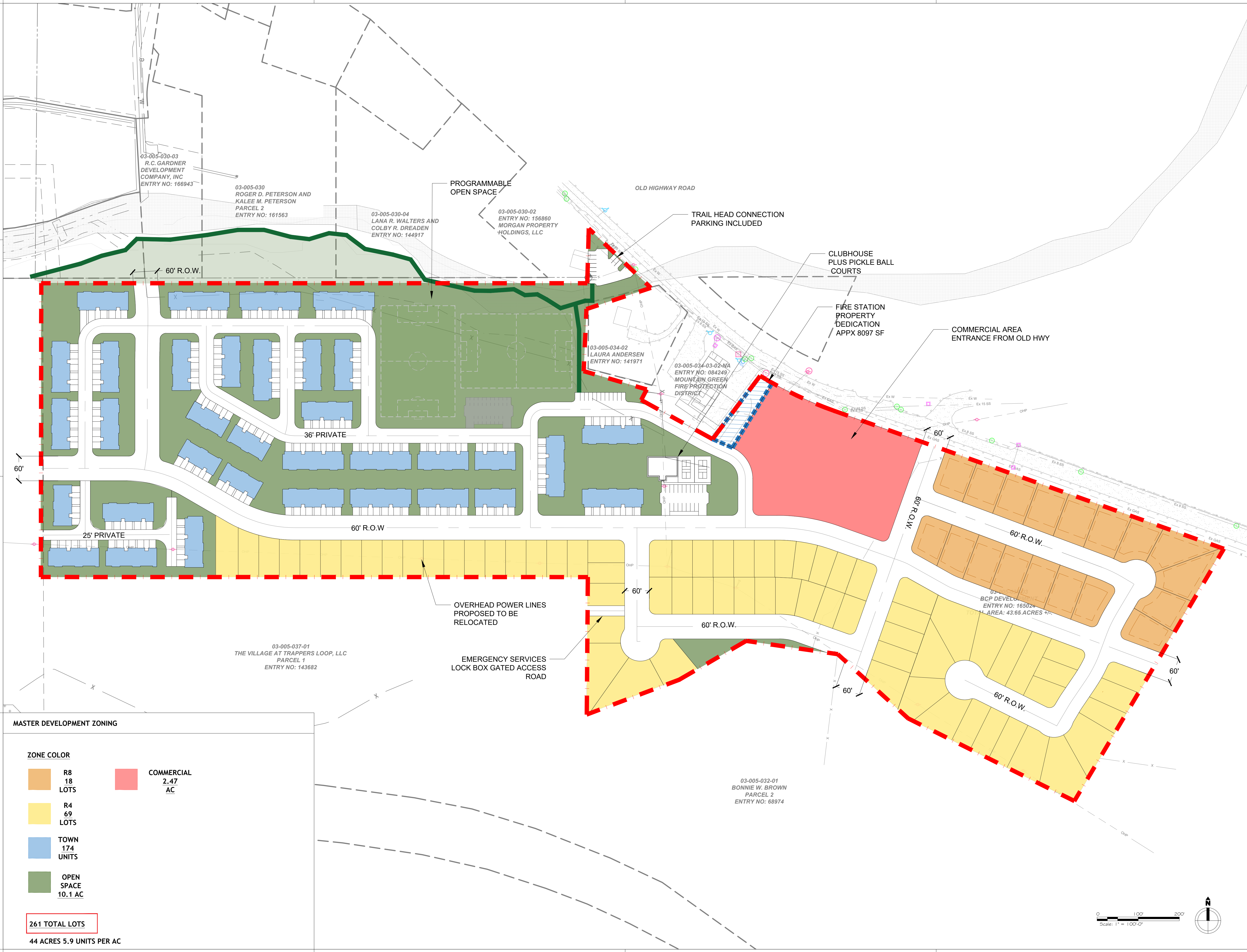
CLUBHOUSE VIEW NORTH



TRAIL

ISSUE

MARK	DATE	DESCRIPTION



WHEN RECORDED RETURN TO:
BCP DEVELOPMENT, LLC.
Attn: Peter Evans
300 S 1350 E St. 2nd Floor
Lehi, UT 84043

Affects Tax Parcel Nos. : 00-0003-3728, 00-0064-0208

DEVELOPMENT AGREEMENT
EAGLE VISTA VILLAS

This Development Agreement ("**Agreement**") is entered into as of ~~July~~August __, 2026 ("**Effective Date**") by and between MORGAN COUNTY, (the "**County**"), a political subdivision of the State of Utah and BCP DEVELOPMENT, LLC., a Delaware limited liability company and its successors, assigns, and transferees as permitted pursuant to this Agreement (the "**Developer**"), as the developer of a mixed-use project known as Eagle Vista Villas (the "Project"), consisting of residential development, neighborhood commercial development, parks, trails and open space, and a dedication of land for a future fire station, to be developed on approximately 43.15 acres of real property as the developer of a mixed-use project known as Eagle Vista Villas (the "Project") to be developed on approximately 44 acres of real property located within the unincorporated boundaries of Morgan County, Utah, as more fully described in **Exhibit A**, attached hereto and incorporated hereby by this reference ("**Property**") in accordance with and pursuant to this Agreement. Developer and the County are referred to in this Agreement individually as a "**Party**" and collectively as the "**Parties**".

RECITALS

- A. Developer owns the Property as more fully described in **Exhibit A**. Developer represents that it is the sole legal and equitable owner of the Property.
- B. On April 21, 2026, the County Commission approved an amendment to Section 155.266 of the Morgan County Land Use Code ("**County Code**") and the Town Center Design Standards which will facilitate development of the Project.
- C. At the request of the Morgan County Commission and pursuant to § 155.266(B)(4) of the County Code, Developer and the owner of the adjacent Gardner Development Town Center property participated in preparing a Joint Conceptual Plan and Narrative ("**Conceptual Plan**") for the coordinated planning and development of their respective Town Center properties. The Gardner Development owner participated in the planning process and represented to the County Commission that it was working cooperatively with Developer and the County in preparing the Conceptual Plan. Following consideration at a duly noticed public meeting, the County Commission approved the Conceptual Plan as the County's coordinated planning framework by Ordinance CO 26 - ____ approving this Project. The approved Conceptual Plan is attached as Exhibit B and incorporated herein.
- D. The Developer also owns an adjacent parcel consisting of approximately 6.29 acres ("**Rezone Area**") that is currently zoned Rural Residential (RR-1) and is not presently located within the Town Center zoning district. At the request of the Morgan County Commission, the Developer agreed to include the adjacent parcel as part of the overall Project in order to provide a detached single-family residential transition between the Town Center development and surrounding development. To accomplish that objective, the Developer has applied

to rezone the adjacent parcel from RR-1 to R1-8, (“**Rezone**”) as depicted on **Exhibit D**, which rezone is intended to be considered and approved contemporaneously with this Agreement as an integral component of the overall Project.

E. The Parties acknowledge that the Conceptual Plan, the Rezone, the commercial-allocation reduction, and this Agreement are related components of the Project but are separate land-use actions subject to independent consideration and approval. Except for the effectiveness of the Rezone as an express condition precedent to the effectiveness of this Agreement, approval of one action is not conditioned upon approval of another. The Parties acknowledge that approval of the Conceptual Plan, approval of the Rezone, and approval of this Agreement are intended to occur concurrently and constitute interrelated components of the overall approval of the Project. Approval of any one of these actions is expressly conditioned upon approval of the others.

Formatted: Font: 11 pt

F. Upon approval, the County finds that the Project, including the approved Conceptual Plan, the Rezone, and this Agreement, is consistent with the Morgan County General Plan, the County Code, applicable Utah law, and the approvals granted concurrently herewith. The County further finds that the Project satisfies the requirements of § 155.266 of the County Code, including the findings necessary to approve the reduction in the commercial allocation.

G. The Parties acknowledge that the Project’s neighborhood commercial component, the Open Space System (as defined in Section 4.6(a) below), and the TC Area Improvements (as defined in Section 4.6(b) below) have been planned and negotiated as an integrated whole, and together implement the purposes and objectives of the Town Center (“TC”) zone under Morgan County Code § 155.266, including the County’s objectives for neighborhood commercial services, parks, trails, open space, and the orderly, coordinated development of the broader TC area as a connected and cohesive district.

The Parties further acknowledge that the Project includes not less than 2.5 acres of land within the Town Center zoning district designated for neighborhood commercial development, located adjacent to the parcel to be dedicated for a future fire station and taking direct access from Old Highway Road, and that this commercial component is a material and negotiated element of the Project and of the approvals granted concurrently herewith.

G. ~~The County further finds that the Project provides substantial, measurable, and enforceable public benefits that support the reduction in the commercial allocation approved herein and materially exceed those that would otherwise be achieved through strict compliance with the Town Center Zone requirements. Such public benefits include, without limitation, dedication of land for a future fire station, dedication of public trail property, construction and enhancement of regional trail connections, construction of recreational amenities, provision of a broader mix of housing types, including detached single family residences, and implementation of coordinated development patterns that promote connectivity, compatibility, and cohesive development within the Town Center area and surrounding properties.~~

H. This Agreement is entered into pursuant to the County Land Use, Development, and Management Act, Utah Code Title 17, Chapter 79 (the “**Act**”).

I. Developer and County have cooperated in the preparation of this Agreement.

J. The Parties understand and intend that this Agreement constitutes a “development agreement” as defined in § 17-79-102(20)(a) of the Act and is entered into pursuant to § 17-79-508 of the Act, each as amended or renumbered from time to time.
~~The Parties understand and intend that this Agreement is a~~

Formatted: Font: 11 pt, Bold

Formatted: Font: Bold

“development agreement” within the meaning of, and entered into pursuant to, the terms of §17-79-102(a) of the Act.

- K. The proposed development of the Property is designed to further the goals and objectives of the County, provide public benefits, and implement the long-range planning vision of the General Plan. The provisions of this Agreement are intended to promote public health, safety, and welfare and advance the policies of the County pursuant to County Code §155.530.
- L. Developer and County enter into this Agreement to define certain standards, clarify expectations, and establish enforceable commitments associated with the development of the Property and Project.

NOW, THEREFORE, in consideration of the foregoing recitals, the mutual promises and covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, County and Developer hereby agree to the following:

AGREEMENT

1. INCORPORATION OF RECITALS AND EXHIBITS

1.1 Incorporation.

The foregoing Recitals and all attached Exhibits are hereby incorporated into this Agreement.

1.2 Conceptual Plan.

The approved Conceptual Plan, attached as **Exhibit B**, is incorporated into this Agreement and is binding upon the Developer and all successors, assigns, and subsequent owners of any interest in the Property. The Conceptual Plan shall run with the Property to the extent applicable to the Property and shall govern the coordinated planning and development of the Property as provided in this Agreement.

The Parties acknowledge that the Conceptual Plan also applies to other property depicted in the Conceptual Plan and provides a coordinated planning framework for property not subject to this Agreement. Each development agreement shall govern only the property to which it applies, and nothing in this Agreement shall impose upon the Developer responsibility for the obligations of any other property owner or make the Developer responsible for another property owner's default under a separate development agreement. Approval or incorporation of the Conceptual Plan does not grant vested rights or development approval to any property owner that has not executed the Conceptual Plan and entered into a development agreement approved by the County or otherwise obtained vested rights under applicable law.

1.3 Order of Precedence.

If any conflict or inconsistency exists between the operative provisions of this Agreement and the Conceptual Plan, Narrative, renderings, plans, or other Exhibits, the operative provisions of this Agreement shall control, except where this Agreement expressly provides that a specifically identified Exhibit provision controls. The Conceptual Plan establishes the approved general development framework for the Project. Except for a standard, quantity, public benefit, deadline, improvement, dedication, or other commitment specifically identified as mandatory in an operative provision of this Agreement, the notes, renderings, dimensions, alignments, lot configurations, phasing boundaries, and other details shown in the Exhibits are conceptual and illustrative and may be refined through the preliminary plat, final plat, engineering, and permit-approval processes without an amendment to this Agreement, provided that the refinement complies with applicable

Formatted: Font: Bold

Formatted: Font: 11 pt

law and does not increase the maximum approved density, authorize an unapproved Residential Product Type, or materially reduce an obligation expressly imposed on Developer by this Agreement. General incorporation of an Exhibit does not, by itself, convert an illustrative detail into an independent obligation or limit the development flexibility expressly granted by this Agreement.

2. ZONING, PERMITTED USES, AND PLAT APPROVAL

2.1 Zoning and Permitted Uses.

The Property is currently zoned Town Center District (“TC”) and Rural Residential (“RR-1”). The Property is also subject to the Town Center Design Standards set forth in §§ 155.265 through 155.270—270 of the County Code. Following approval of the Rezone contemplated by this Agreement, the Property shall consist of TC and R1-8 zoning districts as shown on the approved exhibits.

Within the TC-zoned portion of the Property, not less than two and one-half (2.5) acres shall be designated for neighborhood commercial use as provided in Section 4.7 and as depicted on the Conceptual Plan attached hereto as Exhibit B. Commercial development within the Project shall be subject to the use, design, signage and parking requirements applicable within the TC Zone.

2.2 Preliminary and Final Plats.

The Developer shall obtain approval of all preliminary and final plats required for development of the Property in accordance with §§ 155.405 through 155.424 of the County Code.

2.3 Completion Assurances.

Developer shall provide improvement completion assurance for all required public improvements in accordance with Land Use Code § 155.420 and as set forth in Section 11.3 of this Agreement. No third party, including lot purchasers, shall have rights as a third-party beneficiary under any improvement completion assurance.

2.4 Building Permits.

Following recordation of the applicable final plat(s), Developer may sell lots and apply for building permits in accordance with applicable law. The County shall issue building permits only upon compliance with applicable law, the County Code, this Agreement, approved plats, applicable conditions of approval, and all required infrastructure and financial-assurance requirements. Nothing in this Agreement limits or modifies the County’s authority or procedures under applicable law or the County Code to withhold, deny, suspend, condition, or revoke any permit, certificate, inspection, plat approval, or other development approval.

3. REZONE OF PORTION OF THE PROPERTY

3.1 Rezone Authorization and Agreement.

Contemporaneously with approval of this Agreement, the County Commission separately approved the rezone of the approximately 6.29-acre Rezone Area from RR-1 to R1-8, as depicted and legally described in Exhibit D, by Ordinance No. _____. The Rezone constitutes an integral component of the Project approvals, and this Agreement shall not become effective unless and until the Rezone ordinance becomes effective.

3.2 Independent Land-Use Action. Relationship to Agreement.

The Conceptual Plan, the Rezone, the commercial-allocation reduction, and this Agreement are related components of the Project but constitute separate land-use actions, each subject to independent consideration and approval under applicable law. Approval of the Conceptual Plan shall not be a condition precedent to consideration or approval of the commercial-allocation reduction, and approval of the commercial-allocation reduction shall not be a condition precedent to consideration or approval of the Conceptual Plan. A delay in, challenge to, or failure to approve one such action shall not, by itself, invalidate or impair any other action that has been lawfully approved or any vested right arising from that approval. The Rezone becoming effective is the only condition precedent to this Agreement becoming effective. No additional approval, sequencing requirement, or condition precedent shall be implied from the relationship among these land-use actions. The Rezone, Conceptual Plan, and this Agreement are intended to function together as an integrated approval framework for the Project. The rights and obligations established by this Agreement are based upon approval of the Rezone and Conceptual Plan.

Formatted: Font: 11 pt

3.3 Effect of Rezone.

Upon the effective date of the Rezone ordinance, the Rezone Area shall be governed by the standards applicable to the R1-8 zoning district, together with the applicable provisions of this Agreement and the approved Conceptual Plan.

3.4 Consistency with Approved Development.

Upon the effective date of the Rezone, the Rezone Area shall be governed by the standards, permitted uses, density limitations, and other requirements applicable to the R1-8 zoning district, together with any additional requirements imposed by this Agreement and the approved Conceptual Plan. Nothing in this Agreement modifies or supersedes the requirements of the R1-8 zoning district.

3.5 Scope of Rezone.

The Rezone applies solely to the approximately 6.29-acre Rezone Area depicted and legally described in **Exhibit D** and does not alter the zoning applicable to any other portion of the Property. Any subsequent modification of the zoning classification or boundaries of the Rezone Area shall be considered and acted upon in accordance with applicable law and the County Code.

3.6 Vesting.

Upon the effective date of the Rezone ordinance, the zoning and development rights associated with the Rezone Area shall constitute vested rights under this Agreement, subject only to the terms, conditions, and limitations expressly set forth herein and applicable state law.

4. APPROVED USE, DENSITY, AND DEVELOPMENT STANDARDS

4.1 Property Subject to Agreement.

The Property subject to this Agreement is legally described in **Exhibit A** attached hereto. No additional property shall be added to or removed from this Agreement except with written amendment by the Parties.

4.2 Approved Use, Density, Commercial Allocation and Required Findings.

Developer is vested with the right to develop and construct no more than two hundred ~~seventy sixty seven~~ (270~~267~~) dwelling units within the Project. Developer is authorized, but not required, to develop up to

Formatted: Font: 11 pt

two hundred ~~seventy sixty seven~~ (270~~267~~) dwelling units within the Project. At full buildout, the Project shall contain not fewer than ~~ninety-six (96) one hundred forty three (143)~~ detached single-family dwelling units, consisting of Executive and Signature Single-Family Homes in such proportions as Developer may determine, and not more than one hundred ~~seventy twenty four~~ (174~~124~~) Luxury Townhomes. Subject to those limitations, Developer may adjust the number and mix of dwelling units without amending this Agreement. These requirements apply to the Project as a whole at full buildout and do not establish a minimum total unit count, require the development of any Luxury Townhomes, or require any individual phase to contain a particular unit mix. If an inconsistency exists between this Section and any unit count, allocation, tabulation, illustration, or narrative contained in the Conceptual Plan, this Section controls. ~~-, subject to the required housing mix and all other requirements of this Agreement.~~ The approved dwelling units shall consist only of the following residential product types (“Residential Product Types”):

- (a) Executive detached single-family homes
- (b) Signature detached single-family homes and;
- (c) Luxury townhomes.

Developer may adjust the number of dwelling units within each approved range without amending this Agreement, provided that the total number of dwelling units does not exceed ~~270~~ 267.

For purposes of this Agreement, “dwelling unit” means one dwelling within a Residential Product Type expressly identified and approved under this Section. No apartment, condominium, multifamily configuration, or other residential use or product type not expressly identified in this Section may be developed within the Project without an amendment to this Agreement approved by the County Commission. The term “dwelling unit” does not independently authorize any housing type, building configuration, density, or use not expressly approved by this Agreement and the Conceptual Plan.

~~The Project shall include not less than two and one-half (2.5) acres of land within the TC zoning district designated for neighborhood commercial use, as more fully provided in Section 4.7 (the “Commercial Parcel”). Section 155.266(C) of the County Code would otherwise require that thirty-five percent (35%) of the development area, or approximately 15.10 acres, be designated for commercial uses. The County approves a commercial allocation below that otherwise required by § 155.266(C) based upon the housing mix, the Commercial Parcel provided under Section 4.7, and the other measurable and enforceable public benefits required by this Agreement, and based upon the findings set forth in this Section and in § 155.266(D).~~

~~The minimum commercial development required within the Project is zero (0) square feet of commercial floor area. The County approves a commercial allocation below that otherwise required by § 155.266(C) of the County Code based upon the housing mix and other measurable and enforceable public benefits required by this Agreement.~~

The approved residential density, housing mix, commercial development, ~~park and~~ open space, amenities, trails, and land dedications depicted on the approved Conceptual Plan are incorporated into this Agreement and constitute the approved development program for the Property. The County approves a commercial allocation for the Project that is less than the commercial allocation otherwise required by §155.266(C). The County further finds, based upon substantial evidence contained in the legislative

record, that the approved reduction satisfies the requirements of §155.266(D), including the following finds:

(a) Due to the location, configuration relationship to existing and planned commercial areas, circulation patterns, connectivity, and surrounding development patterns, strict application of the commercial allocation requirement would result in less cohesive Town Center development and could create isolated commercial areas not integrated with other commercial development;

(b) The approved development pattern, together with the public benefits secured through this Agreement, provides a substantially greater and more durable benefit to the County and the Town Center area than strict compliance with the commercial allocation requirement;

(c) Public benefits supporting the reduction include the measurable and enforceable public benefits secured by this Agreement, including, without limitation, dedication of land for a future public fire station, regional trail connectivity and public trail dedications, enhanced recreational amenities, infrastructure and connectivity improvements, provision of diverse housing types including detached single-family residences, landscaping and buffering, and the additional public benefits described in Sections 4.3 through 4.8 and Article 5 of this Agreement.

4.3 Diversity of Housing Types.

As a material public benefit supporting approval of the Conceptual Plan and the reduction in commercial allocation, Developer shall construct each Residential Product Type in the quantities and within the ranges established in Section 4.2.

The Residential Product Types shall satisfy the following requirements:

(a) **Executive and Signature Single-Family Homes.** The Executive and Signature Single-Family Home products within the development shall consist of detached, single-family residential dwelling units designed to an elevated standard of finish and architectural quality, representing the highest residential tier within the Project. The units shall feature distinctive mountain-style architecture incorporating enhanced elements such as stone, accents, articulated and pitched rooflines, and refined exterior materials and color palette intended to harmonize with the surrounding natural setting and to present a distinguished, high-quality streetscape. The homes shall offer a variety of floor plans and elevations to promote visual diversity and reinforce the executive character of the product, while maintaining a unified design theme throughout the Project consistent with the applicable design standards of the County.

(b) **Luxury Townhomes.** The townhome product within the development shall consist of attached, two-story residential dwelling units designed to a luxury standard of finish and architectural quality. The units shall feature mountain-style architecture incorporating elements such as stone, accents, pitched rooflines, and complementary exterior materials and color palette intended to harmonize with the surrounding natural setting and to present a cohesive, high-quality streetscape. The architectural design, materials, and elevations are intended to create an attractive, premium residential offering that appeals to discerning homebuyers while remaining consistent with the character of the community and the applicable design standards of the County.

(c) **Compliance.** All Residential Product Types shall comply with the County's applicable Town Center Design Standards, the approved Conceptual Plan, and the design requirements established by this Agreement. Descriptions of architectural character or quality in this Section do not replace or reduce compliance with objective County design and construction standards.

(d) **Limited Adjustments.** Minor adjustments to individual lot dimensions, dwelling sizes, and lot configurations may be approved through the preliminary and final plat process without amending this Agreement, provided that each adjustment: (i) complies with applicable development standards; (ii) remains substantially consistent with the approved Conceptual Plan; (iii) does not increase the maximum approved density; (iv) does not create or authorize an unapproved Residential Product Type; and (v) does not materially alter the character, quality, or overall housing mix approved by this Agreement.

A proposed modification that does not satisfy all of these requirements is a material modification requiring an amendment to this Agreement approved by the County Commission.

(e) **Housing Mix Within Project Phases.** Each preliminary and final plat application shall identify the number and type of dwelling units included within the proposed phase and demonstrate how the proposed phase, together with completed and remaining development, will satisfy the required maximum allocations established by Section 4.2.

(f) **Final Phase.** The County shall not approve the final residential phase or issue a certificate of occupancy for a dwelling unit that would cause the Project to exceed an approved maximum under Section 4.2.

4.4 Community Landscaping, Signage, and Buffers.

As a material public benefit supporting the approved reduction in the commercial allocation, and to enhance the character, appearance, and character of the TC portion of the Project, Developer shall provide, at Developer's sole cost and expense, community landscaping and entry features for the Project, including street and park-strip landscaping, perimeter landscaping and buffers between differing housing types and adjacent uses, street trees along the main roadway, and monument, entry, and wayfinding signage consistent with County regulations and the County's TC Zone standards. Such landscaping, signage, and buffer improvements shall be owned and maintained by one or more Owner Associations (defined below) in accordance with recorded CC&Rs, at no cost or expense to the County.

4.5 Construction-Phase Commitments.

In addition to the public benefits provided elsewhere in this Agreement, and in recognition of the impacts of construction on existing residents and the surrounding community, Developer shall implement reasonable construction-management practices during development of the Project, including: (a) fugitive dust control measures consistent with applicable air-quality requirements; (b) designation and use of haul routes and truck-traffic management intended to minimize impacts on existing residential streets and neighboring properties; (c) observance of reasonable construction hours consistent with County requirements and applicable noise standards; and (d) maintenance of construction sites in a manner that reasonably controls mud, debris, and tracking onto public roadways. The specific measures shall be consistent with the County's applicable ordinances and any conditions of approval for the Project.

~~4.6 Infrastructure, Open Space Improvements Serving the Broader Town Center Area.~~

~~As a further material public benefit supporting the approved reduction in the commercial allocation, in addition to the trail improvements described in Section 6.1, Developer shall provide certain roadway, access, utility, water, and open space improvements and dedications that are designed and sized to serve~~

not only the Project but also the broader TC area as set forth in the Conceptual Plan attached hereto as **Exhibit B**, thereby supporting the orderly, coordinated development of the TC area as a connected and cohesive district. Except as otherwise expressly provided in this Agreement, including the cost recovery provisions applicable to oversized utility infrastructure set forth in subsection (c) below, the improvements described in Section 4.6 shall be designed and constructed by Developer at Developer's sole cost and expense.

~~(a) Roadway and Access Improvements.~~ Developer shall design and construct roadway and access improvements within and adjacent to the Project that improve vehicular and pedestrian circulation for the TC area to provide an improved access route for the benefit of other developments within the TC Zone as set forth in the Conceptual Plan attached hereto as **Exhibit B**. These improvements are intended to reduce the future access and circulation burden on neighboring parcels and to support the connectivity of the TC area as contemplated by the County's planning for the area. In connection with the foregoing, and as anticipated by the approved Conceptual Plan, Developer shall dedicate to the County or the applicable roadway authority such right of way along Old Highway Road as shown on the concept street layout in the Conceptual Plan attached hereto as **Exhibit B**. The specific location, configuration, and dimensions of such roadways and access improvements shall be established through the preliminary and final plat process.

~~(b) Reciprocal and Cross Access.~~ Developer shall grant and record such reciprocal access and cross access easements as are reasonably necessary to provide for vehicular and pedestrian access to and from neighboring parcels, including, as applicable, the adjacent parcels currently owned by Cottonwood Meadows Holdings, Soderby LTD, Bonnie W. Brown, Bar Z Investments, and Village at Trappers Loop LLC, thereby supporting the orderly development and connectivity of adjacent properties within the Town Center area. The specific location, configuration, and terms of such easements shall be established through the preliminary and final plat process and the applicable access or exchange agreements.

~~(c) Utility Infrastructure with Broader Area Capacity.~~ Developer shall, at its sole cost, design and construct all utility infrastructure required to serve the Project in accordance with applicable law and the requirements of the applicable utility providers. If an applicable utility provider requires infrastructure to be oversized or extended beyond that reasonably necessary to serve the Project, any reimbursement, credit, cost sharing arrangement, or other cost recovery mechanism may be established through a separate written agreement with the utility requiring the additional capacity. If the County requests additional capacity or infrastructure beyond that required by applicable law, the County Code, generally applicable County standards, approved plans, conditions of approval, or applicable utility provider requirements, any County participation shall arise only through a separate written agreement approved by the County Commission.

~~(d) Water Rights and Share Dedication.~~ As a public benefit, Developer shall dedicate or convey to the applicable culinary water and secondary (irrigation) water providers such water rights and water shares as are legally required to serve the Project, in the quantities and through the mechanism required by the applicable provider and in accordance with applicable Utah law, thereby protecting the capacity of the existing water systems for the benefit of current and future residents of Mountain Green. The specific water rights, shares, and dedication mechanism shall be established in coordination with the applicable provider and in accordance with its water dedication and share requirement policies and applicable Utah law.

~~(e) Shared Open Space and Regional Trail Connectivity.~~ The open space, trail, and pedestrian improvements provided by Developer under this Agreement, including the Cottonwood Creek Trail and the trailhead, easements,

and related improvements described in Section 6.1, are intended to be publicly accessible and to provide connectivity that benefits the broader Mountain Green and TC area. Developer shall cooperate in good faith with the County in coordinating the location and configuration of these improvements so that they may be extended through, and connected to, future development and public open space within the TC area. Nothing in this Section shall be construed to obligate Developer to construct, fund, secure, or complete any trail improvement beyond those located within the Property and expressly described in Section 6.1, and the foregoing statement of intent shall not be enforceable as an affirmative obligation of Developer.

4.6. Park, Open Space, and Infrastructure Improvements Serving the Broader Town Center Area,

As a further material public benefit supporting the approved reduction in the commercial allocation, and in addition to the improvements described in Section 6.1, Developer shall provide the parks, trails, open space, roadway, access, utility, and water improvements and dedications described in this Section 4.6, which are designed and sized to serve not only the Project but also the broader TC area as set forth in the Conceptual Plan attached hereto as Exhibit B, thereby supporting the orderly, coordinated development of the TC area as a connected and cohesive district.

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: (Default) Times New Roman

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

(a) Open Space System; Local Park and Trail Areas,

As a material public benefit to the TC zone and to the Mountain Green community as a whole, Developer shall provide not less than ten (10) acres of parks, trails, and open space within the Project (collectively, the “Open Space System”), consisting of: (i) approximately six (6) acres of publicly accessible park and trail improvements, including the local park and the Cottonwood Creek Trail corridor, in the general locations depicted on the Conceptual Plan attached hereto as Exhibit B and as further described in Section 6.1 (the “Local Park and Trail Areas”), which shall be open and accessible to the general public and shall not be restricted to residents of the Project; and (ii) approximately four (4) acres of common open space, landscaped areas, and pedestrian connections distributed throughout the Project (the “Neighborhood Open Space”), which shall be owned and maintained by one or more Owner Associations for the benefit of Project residents. Together, the Open Space System is designed to function as an integrated network of active and passive open space serving both the Project and the broader TC area, providing recreational opportunities, trail connectivity to the Cottonwood Creek Trail corridor, and pedestrian linkages between the Project’s residential neighborhoods, the Commercial Parcel, and adjacent TC parcels, thereby advancing the TC zone’s purpose of creating a walkable, connected, and cohesive district,

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

(b) TC Area Improvements,

In addition to the Open Space System, Developer shall provide the roadway, access, utility, and water improvements and dedications described in subsections (b)(1) through (b)(4) below (collectively, the “TC Area Improvements”), which are designed and sized to serve not only the Project but also the broader TC area as set forth in the Conceptual Plan, thereby supporting the orderly, coordinated development of the TC area as a connected and cohesive district,

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

(1) Roadway and Access Improvements,

Developer shall design and construct roadway and access improvements within and adjacent to the Project that improve vehicular and pedestrian circulation for the TC area to provide an improved access route for the benefit of other developments within the TC Zone as set forth in the Conceptual Plan

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

attached hereto as Exhibit B. These improvements are intended to reduce the future access and circulation burden on neighboring parcels and to support the connectivity of the TC area as contemplated by the County’s planning for the area. In connection with the foregoing, and as anticipated by the approved Conceptual Plan, Developer shall dedicate to the County or the applicable roadway authority such right-of-way along Old Highway Road as shown on the concept street layout in the Conceptual Plan attached hereto as Exhibit B. The specific location, configuration, and dimensions of such roadways and access improvements shall be established through the preliminary and final plat process.

(2) Reciprocal and Cross-Access,

Developer shall grant and record such reciprocal access and cross-access easements as are reasonably necessary to provide for vehicular and pedestrian access to and from neighboring parcels, including, as applicable, the adjacent parcels currently owned by Cottonwood Meadows Holdings, Soderby LTD, Bonnie W. Brown, Bar-Z Investments, and Village at Trappers Loop LLC, thereby supporting the orderly development and connectivity of adjacent properties within the Town Center area. The specific location, configuration, and terms of such easements shall be established through the preliminary and final plat process and the applicable access or exchange agreements.

(3) Utility Infrastructure with Broader-Area Capacity,

Developer shall, at its sole cost, design and construct all utility infrastructure required to serve the Project in accordance with applicable law and the requirements of the applicable utility providers. If an applicable utility provider requires infrastructure to be oversized or extended beyond that reasonably necessary to serve the Project, any reimbursement, credit, cost-sharing arrangement, or other cost-recovery mechanism may be established through a separate written agreement with the utility requiring the additional capacity. If the County requests additional capacity or infrastructure beyond that required by applicable law, the County Code, generally applicable County standards, approved plans, conditions of approval, or applicable utility-provider requirements, any County participation shall arise only through a separate written agreement approved by the County Commission.

(4) Water Rights and Share Dedication,

As a public benefit, Developer shall dedicate or convey to the applicable culinary water and secondary (irrigation) water providers such water rights and water shares as are legally required to serve the Project, in the quantities and through the mechanism required by the applicable provider and in accordance with applicable Utah law, thereby protecting the capacity of the existing water systems for the benefit of current and future residents of Mountain Green. The specific water rights, shares, and dedication mechanism shall be established in coordination with the applicable provider and in accordance with its water-dedication and share-requirement policies and applicable Utah law.

(c) Shared Open Space and Regional Trail Connectivity,

The open space, trail, and pedestrian improvements provided by Developer under this Agreement, including the Cottonwood Creek Trail and the trailhead, easements, and related improvements described in Section 6.1, are intended to be publicly accessible and to provide connectivity that benefits the broader Mountain Green community and TC area. Developer shall cooperate in good faith with the County in coordinating the location and configuration of these improvements so that they may be extended through, and connected to, future

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

development and public open space within the TC area. Nothing in this subsection shall be construed to obligate Developer to construct, fund, secure, or complete any trail improvement beyond those located within the Property and expressly described in Section 6.1, and the foregoing statement of intent shall not be enforceable as an affirmative obligation of Developer.

Formatted: Font: 11 pt

(d) Ownership; Public Access; Maintenance.

Formatted: Font: (Default) Times New Roman, 11 pt

The Local Park and Trail Areas shall be owned and maintained by one or more Owner Associations in perpetuity, subject to a public access easement in a form reasonably acceptable to the County, which easement shall be recorded against the applicable parcels at or before recordation of the final plat for the phase containing such improvements. All costs of maintenance, repair, and replacement of the Open Space System shall be funded through the Owner Associations as provided in Section 7.3 of this Agreement, at no cost to the County. Developer and each Owners Association voluntarily agree, pursuant to this Agreement, to own and maintain the Local Park and Trail Areas and the other publicly accessible portions of the Open Space System, and the County has not required, and this Agreement shall not be construed as the County requiring, private maintenance of a public amenity except as voluntarily agreed in this Agreement.

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

(e) Completion.

Formatted: Font: 11 pt

Developer shall achieve substantial completion of the Local Park and Trail Areas (or such phases thereof as are depicted on Exhibit B) in accordance with the amenity phasing and completion schedule set forth in Section 5.2 of this Agreement. Neighborhood Open Space within each phase shall be substantially completed concurrently with the subdivision improvements for such phase, consistent with the completion assurance provisions of Section 10.3 of this Agreement and Morgan County Code § 155.420.

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

(f) County Findings.

Formatted: Font: 11 pt

The County acknowledges and finds that the Open Space System and the TC Area Improvements: (i) constitute substantial and material public benefits to the TC zone and to the Mountain Green community; (ii) meet or exceed the open space, amenity, and community design requirements of Morgan County Code §§ 155.265 through 155.270 applicable to the Project; (iii) with respect to the Local Park and Trail Areas, provide publicly accessible recreational amenities and trail connectivity serving residents and properties throughout the broader TC area; (iv) with respect to the Neighborhood Open Space, implement the open space, landscaping, and walkability objectives of the TC zone, reduce demand on public park facilities, and establish the pedestrian framework connecting the Project's residential neighborhoods to the Local Park and Trail Areas and the Commercial Parcel; (v) with respect to the TC Area Improvements, reduce the future access, circulation, utility, and water-supply burden on neighboring parcels and support the orderly and coordinated development of the TC area; and (vi) together with the other obligations of Developer under this Agreement, constitute good and valuable consideration for the vested rights and approvals granted to Developer under this Agreement.

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

(g) Cost; Cost Recovery.

Formatted: Font: 11 pt

Except as otherwise expressly provided in this Agreement, including the cost-recovery provisions applicable to oversized utility infrastructure set forth in subsection (b)(3) above, the Open Space System and the TC

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Area Improvements shall be designed and constructed by Developer at Developer's sole cost and expense. Developer waives any claim to impact fee credits or reimbursement for the Local Park and Trail Areas, which waiver the County acknowledges as an additional public benefit under subsection (f) above.

Formatted: Font: 11 pt

4.7 4.7 Neighborhood Commercial Parcel.

(a) Commercial Parcel. As a material component of the Project and of the approved development program, the Project shall include not less than two and one-half (2.5) acres of land within the Town Center zoning district designated for neighborhood commercial use (the "Commercial Parcel"). The Commercial Parcel shall be located adjacent to the FD Parcel described in Section 6.3 and shall have frontage upon Old Highway Road, in the general location depicted on the Conceptual Plan attached hereto as Exhibit B. The specific boundaries, configuration and dimensions of the Commercial Parcel shall be established through the preliminary and final plat process, provided that the Commercial Parcel shall in all events contain not less than 2.5 acres.

(b) Permitted Uses; Compliance with TC Zone; Use Not Determined by This Agreement. The uses permitted on the Commercial Parcel shall be those commercial uses authorized within the Town Center zoning district under § 155.132 of the County Code, and all development and operation of any business upon the Commercial Parcel shall comply with the requirements applicable within the TC Zone, including the Town Center Design Standards set forth in §§ 155.265 through 155.270 of the County Code and the County's generally applicable signage and off-street parking requirements. The Parties acknowledge and agree that the specific commercial use or uses to be developed upon the Commercial Parcel are not determined by this Agreement and shall be established through the site plan, subdivision and permitting processes applicable at the time of development, in accordance with the County Code and applicable law. Nothing in this Agreement obligates Developer or any successor owner to develop, or restricts Developer or any successor owner from developing, any particular commercial use otherwise permitted within the TC Zone, and no amendment to this Agreement shall be required in order to pursue approval of any such permitted use.

(c) Pad-Ready Delivery; No Vertical Construction Obligation. Developer shall create the Commercial Parcel as a separate legal lot by recorded final plat and shall, at Developer's sole cost and expense, deliver the Commercial Parcel in a pad-ready condition. For purposes of this Agreement, "pad-ready" means that the Commercial Parcel has been rough graded in accordance with the approved construction drawings; that culinary water, sanitary sewer, storm drainage, and dry utilities have been stubbed to the boundary of the Commercial Parcel in capacities adequate to serve commercial development permitted within the TC Zone; and that vehicular access to the Commercial Parcel has been provided directly from Old Highway Road in accordance with the requirements of the applicable roadway authority.

Developer shall not be obligated to construct any vertical improvement or building upon the Commercial Parcel, to design any building, to secure any tenant, occupant, purchaser or user, or to achieve any level of occupancy or commercial activity. Neither the absence of vertical construction upon the Commercial Parcel, nor the absence of any tenant, occupant or user, nor the timing of any future commercial development, shall constitute a default under this Agreement, and no building permit, plat approval, inspection, or certificate of occupancy for any residential dwelling unit or other portion of the Project shall be withheld, denied, suspended, conditioned or delayed on account of any of the foregoing.

Any improvement completion assurance required under Section 10.3 and § 155.420 of the County Code with respect to the Commercial Parcel shall extend only to the pad-ready improvements described in this subsection (c) that Developer is obligated to construct, and shall not extend to any vertical improvement.

(d) Access. The Commercial Parcel shall take direct vehicular access from Old Highway Road and shall not take general vehicular access from the internal street network of the Project. The location and configuration of the access shall be established through the preliminary and final plat process and shall be subject to the approval and permitting requirements of the applicable roadway authority. Nothing in this subsection precludes pedestrian connections between the Commercial Parcel and the Project, or an emergency access connection if required by the applicable fire authority.

(e) Conveyance; Responsibility for Vertical Development. Developer may sell, convey, ground lease or otherwise transfer the Commercial Parcel to any third party at any time. Following delivery of the Commercial Parcel in pad-ready condition, the design, construction, use and operation of any vertical improvement upon the Commercial Parcel shall be the sole responsibility of the then-current owner of the Commercial Parcel, and Developer shall have no continuing obligation or liability with respect thereto. The obligations of this Section 4.7 relating to the designation of the Commercial Parcel for commercial use and to compliance with the TC Zone shall run with the Commercial Parcel and bind each successor owner.

(f) No Conversion Without Amendment. The Commercial Parcel shall not be converted to residential use, reduced below 2.5 acres, or eliminated from the Project except by amendment to this Agreement approved by the County Commission. The dwelling units authorized by Section 4.2 may not be relocated onto the Commercial Parcel, and no portion of the Commercial Parcel shall be counted toward satisfaction of the Open Space System required by Section 4.6.

(g) Exclusion from Owners Association. The Commercial Parcel shall not be included within, and shall not be subject to the jurisdiction, governing documents, architectural review, or assessments of, any Owners Association established pursuant to Article 7 of this Agreement. No Owners Association shall have any obligation to own, operate, maintain, repair or replace any improvement located upon the Commercial Parcel, and the owner of the Commercial Parcel shall have no right to use any Project Amenity reserved for the use of residents and guests of the Project. Because the Commercial Parcel takes direct access from Old Highway Road as provided in subsection (d), the owner of the Commercial Parcel shall have no obligation to contribute to the maintenance of the private roadways within the Project. If the Commercial Parcel is served by a stormwater facility shared with the Project, Developer shall cause to be recorded, at or before recordation of the final plat creating the Commercial Parcel, a drainage easement and maintenance cost-sharing agreement allocating a proportionate share of the maintenance cost of such shared facility to the owner of the Commercial Parcel, at no cost or expense to the County.

Notwithstanding the exclusion of the Commercial Parcel from each Owners Association, the Commercial Parcel remains subject to this Agreement, and this Agreement shall run with and bind the Commercial Parcel and each successor owner thereof as provided in Section 13.1.

(h) Public Benefit. The provision of the Commercial Parcel constitutes a material public benefit supporting approval of the Conceptual Plan, the Rezone, the reduction in the commercial allocation approved pursuant to § 155.266(D), and this Agreement. The County finds that the Commercial Parcel, by reason of its location adjacent to the FD Parcel, its direct access from Old Highway Road, and its relationship to existing and planned commercial areas within the TC Zone, supports the development of the Town Center area as a connected and cohesive district and provides for neighborhood commercial services to residents of the Project and the surrounding Mountain Green community.

~~{Reserved}.~~

4.8 [Reserved].

4.9 Short-Term Rental Prohibition.

As a further material public benefit supporting the approved reduction in the commercial allocation, the Parties acknowledge that the preservation of the Project as a long-term residential community is a material consideration supporting the County's approval of the reduction in commercial allocation.

Short-term rentals, including nightly or transient lodging accommodations, are strictly prohibited within the legally recorded boundaries of the development and shall not be permitted under any circumstances through plat notes, covenants, or other recorded instruments. Allowed uses and development approvals shall be governed by the TC Zone and the County Code and shall proceed through subdivision and building permit approvals consistent with such regulations.

The prohibition against short-term rentals established by this Agreement shall be included in the recorded CC&Rs and shall run with the applicable portions of the Property. Following recordation of the CC&Rs, the prohibition shall bind the Owners Association, each owner of an affected lot or dwelling unit, and their respective successors and assigns. Developer shall be responsible for compliance only with respect to property then owned or controlled by Developer and shall not be liable for a violation committed by an Owners Association, an owner, occupant, tenant, or other third party. The County may enforce the prohibition directly against the person or entity committing or responsible for the violation pursuant to this Agreement and applicable law, subject to any applicable notice-and-cure requirements. Nothing in this provision requires Developer to guarantee enforcement by an Owners Association or to pursue enforcement against another owner.

Formatted: Font: 11 pt

4.10 Applicability of Town Center Development Standards

Except as expressly modified by this Agreement, development of the Property shall comply with the applicable development standards of the TC Zone, including § 155.267 of the County Code, to the extent such standards are not inconsistent with the approved commercial allocation, the approved Conceptual Plan, the Rezone, or the provisions of this Agreement. Development of the Commercial Parcel shall comply with the Town Center Design Standards, including §§ 155.267 and 155.269 of the County Code, as provided in Section 4.7(b).

5. PROJECT AMENITIES

5.1 Project Amenities.

The Project Amenities described in this Section 5.1 constitute material public benefits supporting approval of the Conceptual Plan, the reduction in commercial allocation authorized pursuant to §155.266(D), the Rezone, and this Agreement. The Parties acknowledge that such amenities exceed minimum development requirements and form part of the consideration supporting the approvals granted herein.

- (a) **Amenities.** Developer shall construct the following resident-serving amenities (“**Project Amenities**”).
- Community clubhouse with meeting space, restrooms, and kitchen facilities.

- Community amenities (pickleball court(s) with fencing and safety features.
- Tot lot/playground.
- Covered pavilion with picnic tables.
- Landscaping and water-wise irrigation for all common areas.
- Decorative monument signage at the entrances into the Project.

The amenities described in this Section are voluntarily provided and exceed minimum County subdivision requirements for TC Zone, constituting public benefits associated with the development.

For clarity, the Project Amenities described above shall include: a community clubhouse containing a kitchen area, an open dining and gathering area, a weight room, and restroom facilities, sized sufficiently to support the number of residential and townhome units approved for the Project; two (2) pickleball courts, one (1) of which shall be open and accessible to the general public of Mountain Green, with the remaining court reserved for the use of residents of an Owners Association; a hot tub for the use of residents of the Owner's Association; a large grassed community park improved with shade trees and a children's playground; two (2) neighborhood pocket parks, each improved with seating; a continuous six-foot (6') wide sidewalk along the main roadway through the Project for safe pedestrian circulation; and a reasonable number of public parking stalls in the vicinity of the clubhouse, trailhead, and publicly accessible pickleball court to serve members of the public using the public amenities, in the quantity and configuration to be established through the site plan and subdivision approval process.

Except for the public park, public sidewalk, the publicly accessible pickleball court, the public parking stalls, and the Cottonwood Creek Trail (collectively, the "**Public Amenities**"), which shall be open to the public, the Project Amenities are reserved for the use of residents and guests of the Project. All Project Amenities, including the Public Amenities, shall be owned, operated, maintained, repaired, and replaced by one or more Owner Associations (defined below) in accordance with recorded CC&Rs, at no cost or expense to the County, with the Developer responsible for maintenance until the applicable Owners Association assumes responsibility. Notwithstanding the foregoing, the County and an Owner's Association may, at the County's election and upon mutual written agreement, provide for the County to assume ownership and/or maintenance of one or more of the Public Amenities at such time as the County determines it has the resources and ability to adequately maintain them; provided that, unless and until such a transfer is completed by written agreement ~~and the County's~~, an Owner's Association shall remain responsible for the ownership and maintenance of all Project Amenities, including the Public Amenities.

(b) **County Standards.** Project Amenities shall be built to County standards which are subject to permitting and plan approval. The Developer shall obtain all necessary permits, inspections, and approvals from the County and all applicable regulatory agencies prior to commencement of construction of such Project Amenities.

(c) **Design and Sizing.** Final design, sizing, and placement of the Project Amenities shall be confirmed during the final plat process; provided, however, that no material reduction in the type, function, capacity, or quality of the Project Amenities shall occur without approval of the County in accordance with the County Code.

(d) **Recreational Use Liability; Public Access; Change in Law.**

Formatted: Highlight

(i) Applicability of Recreational Use Protections. The Parties acknowledge that the Developer's agreement to construct, own, maintain, and permit public access to the trail system, including the Cottonwood Creek Trail (collectively, the "**Trail System**"), is based upon the liability protections afforded to private landowners under Utah Code Ann. §§ 57-14-101 through 57-14-205 and § 57-14-401, as amended from time to time, together with any successor statutes or other laws providing substantially equivalent liability protections (collectively, the "**Protection Statutes**"). The Developer, any applicable owner's association, and any successor owner of any portion of the Trail System are collectively referred to as the "**Trail Owner**."

(ii) Public Access and Reasonable Rules. Except as expressly provided in this subsection, the Trail System shall remain open and accessible to the general public. The Trail Owner may adopt and enforce reasonable, nondiscriminatory rules governing use of the Trail System, including reasonable hours of operation, temporary closures for maintenance, repair, hazardous conditions, emergencies, or special circumstances, and the installation and use of gates or other reasonable access-control measures. Any such rules or restrictions shall apply reasonably to both Project residents and members of the general public and shall not be used to defeat or materially impair the public-access obligation imposed by this Agreement. The Trail Owner shall provide the County with a copy of any generally applicable rules governing public use of the Trail System and shall post applicable hours and restrictions at trail access points.

(iii) Preservation of Statutory Protections. The Parties intend that authorized public recreational use of the Trail System qualify for the fullest liability protections available under the Protection Statutes. Nothing in this Agreement shall be construed as creating a duty of care, warranty, representation, special relationship, or assumption of liability beyond that imposed by applicable law or as waiving any protection, limitation of liability, immunity, or defense otherwise available to the County or the Trail Owner.

(iv) Qualifying Change in Law. For purposes of this subsection, a "Qualifying Change in Law" means the repeal, material amendment, or binding judicial interpretation of the Protection Statutes that materially diminishes or eliminates the liability protections applicable to a Trail Owner arising from public recreational use of the Trail System. A change in insurance cost or availability, standing alone, does not constitute a Qualifying Change in Law.

(v) Notice and Temporary Suspension of Public Access. If the Trail Owner reasonably determines that a Qualifying Change in Law has occurred and materially increases the Trail Owner's potential liability arising from public recreational use of the Trail System, the Trail Owner shall provide written notice to the County identifying:

1. the specific statutory amendment, repeal, or binding judicial decision constituting the Qualifying Change in Law;
2. the liability protection materially diminished or eliminated;
3. the resulting material increase in potential liability; and
4. the access restrictions or closure the Trail Owner believes are reasonably necessary in response.

Upon delivery of the written notice, the Trail Owner may temporarily suspend or reasonably restrict public access to the Trail System without being in default under this Agreement. Any suspension or restriction shall be limited to the extent reasonably necessary to address the increased liability resulting from the Qualifying Change in Law.

(vi) Meet and Confer. Within thirty (30) days after the County receives notice under subsection (v), the County and the Trail Owner shall meet and confer in good faith to determine whether public access may reasonably continue through revised operating rules, access restrictions, risk-management measures, transfer of ownership or maintenance responsibility, an amendment to this Agreement, or another mutually acceptable arrangement. Neither Party shall be required to assume additional liability, incur additional expense, transfer or accept ownership, or enter into an amendment without its separate written agreement.

(vii) Continued Suspension During Qualifying Change in Law. If the Parties do not reach a mutually acceptable written agreement, the Trail Owner may continue to suspend or restrict public access only for so long as the Qualifying Change in Law remains in effect and continues to materially diminish the liability protections applicable to the Trail Owner. Such suspension or restriction shall not eliminate, release, or terminate the public-access covenant established by this Agreement.

(viii) Restoration of Public Access. If the Protection Statutes are subsequently reenacted, amended, replaced, or authoritatively interpreted so that the materially diminished liability protection is restored or substantially equivalent protection again becomes applicable to the Trail Owner, the Trail Owner shall reopen the Trail System to the general public within thirty (30) days after the protection becomes effective. The Trail Owner shall thereafter continue to provide public access in accordance with this Agreement, subject to the reasonable rules and restrictions authorized by subsection (ii).

(ix) No County Defense, Indemnification, or Reimbursement. The County shall have no obligation to defend, indemnify, or hold harmless the Developer, a Trail Owner, an Owners Association, or any other private person or entity from claims arising from the ownership, operation, maintenance, condition, or use of the Trail System. The County shall also have no obligation to reimburse any Trail Owner for insurance premiums, deductibles, self-insured retention, loss of insurance availability, risk-management expenses, attorneys' fees, or other costs associated with ownership, maintenance, or public use of the Trail System.

(x) Optional Transfer to County. Following a Qualifying Change in Law, the County may, but shall not be obligated to, consider accepting ownership, operation, or maintenance responsibility for all or any portion of the Trail System. Any transfer or assumption of responsibility shall require a separate written agreement approved by the Morgan County Commission that expressly establishes the property interest transferred and the respective responsibilities and liabilities of the County and the Trail Owner. No County responsibility shall arise unless and until that separate agreement is fully executed and the applicable property interest is conveyed and accepted.

(xi) Covenant Running with the Land. The public-access obligation and the provisions of this subsection shall run with the land and bind the Developer, each applicable owner's association, each Trail Owner, and their respective successors and assigns. A temporary suspension or restriction authorized by this subsection shall not extinguish the public-access obligation or remove the covenant from the Property.

5.2 Amenity Phasing and Completion Schedule.

The Parties acknowledge that the Project is anticipated to be developed in approximately three phases and that phases may proceed concurrently or in an overlapping sequence based upon market demand for the different Residential Product Types.

The following Project-wide amenities shall be constructed as part of the first phase of the Project (For purposes of this Section, “first phase” means the first residential final plat recorded for any portion of the Project):

1. the community clubhouse, including the kitchen, dining and gathering area, weight room, and restroom facilities;
2. the hot tub;
3. both pickleball courts, including the publicly accessible pickleball court;
4. the principal tot lot/playground;
5. the covered pavilion and picnic facilities;
6. the large grassed community park and required shade trees;
7. the Cottonwood Creek Trail and trailhead;
8. the public parking required to serve the clubhouse, trailhead, and publicly accessible pickleball court; and
9. all landscaping, irrigation, sidewalks, pedestrian connections, utilities, and other improvements necessary for the foregoing amenities to be complete, functional, accessible, and available for their intended use.

All Project-wide amenities listed above shall be completed, approved, and available for their intended use before issuance of Certificates of Occupancy for more than fifty percent (50%) of the dwelling units approved within the Project. Concurrent or overlapping development of another phase shall not extend or otherwise modify this requirement.

During each subsequent phase of development, all amenities serving or located within that phase, including any neighborhood pocket park, green space, sidewalk, trail connection, landscaping, and irrigation, shall be completed, approved, and available for their intended use before issuance of Certificates of Occupancy for more than fifty percent (50%) of the dwelling units approved within that phase.

Decorative monument signage at each Project entrance shall be installed before issuance of the first Certificate of Occupancy served by that entrance. If weather prevents timely completion of required landscaping, the County may approve completion during the next appropriate planting season, provided Developer posts financial assurance acceptable to the County and completes the landscaping by a date approved in writing by the County.

The County may withhold Certificates of Occupancy exceeding an applicable phase-specific threshold established by this Section until the required amenities have been completed, approved, and made available for their intended use.

The Commercial Parcel described in Section 4.7 is not a Project Amenity and is not subject to the amenity phasing and completion thresholds established by this Section 5.2.

5.3 No Substitution Without Approval.

Subject to Section 5.1(d), no Project Amenity identified in this Agreement may be eliminated, materially reduced, relocated, or substituted without written approval of the County. In reviewing any proposed modification, the County may consider whether the proposed change would materially affect the public benefits supporting approval of the Conceptual Plan, reduction in commercial allocation, Rezone, or this Agreement.

5.4 Aviation Easement.

All final plats shall include an aviation easement in favor of the County Airport for aircraft operations in airspace over the Property.

6. DEDICATION OF TRAIL OPEN SPACE AND LAND FOR FIRE DEPARTMENT

6.1 Park, Trail, and Open Space Improvements.

Developer shall design, construct, and install the Open Space System described in Section 4.6(a), consisting of the Local Park and Trail Areas and the Neighborhood Open Space, in the general locations depicted on Exhibit B. Improvements within the Local Park and Trail Areas shall include a six-foot (6') wide asphalt pedestrian trail along the Cottonwood Creek corridor substantially in the location shown on Exhibit F (the 'Cottonwood Creek Trail'), together with a trailhead providing access from Old Highway Road, benches, shaded rest areas, directional and public-access signage, and the public parking required by Section 5.1. The Open Space System described in this Section 6.1 and in Section 4.6(a) constitutes a single obligation of not less than ten (10) acres in the aggregate, and nothing in this Agreement shall be construed to require parks, trails, or open space in excess of the Open Space System except as expressly stated herein.

Formatted: Font: 11 pt

Formatted: Font: (Default) Times New Roman, 11 pt

Formatted: Font: 11 pt

6.1 Trail Open Space Dedication.

~~Developer shall, at its sole cost and expense, design and construct a six-foot (6') wide asphalt pedestrian trail along the Cottonwood Creek corridor substantially in the location shown on the Conceptual Plan and Exhibit F (the "Cottonwood Creek Trail"). The Cottonwood Creek Trail improvements shall include a trailhead providing access from Old Highway Road, benches, shaded rest areas, directional and public-access signage, and the public parking required by Section 5.1.~~

The Cottonwood Creek Trail, trailhead, and related improvements shall remain privately owned and, except as authorized by Section 5.1(d), shall remain open and accessible to the general public. Developer and the applicable owners association shall own, operate, maintain, repair, and replace the trail and related improvements at no cost to the County.

Developer shall record a permanent public-access easement for the Cottonwood Creek Trail ("Trail Easement") Before recordation of the first final plat affecting the Cottonwood Creek Trail, Developer shall record a permanent public access easement over Cottonwood Creek Trail ("Trail Easement") as shown on Exhibit F in a form reasonably and mutually acceptable to the Parties, including the County Attorney and recordable against the Property, sufficient to provide for public access to and maintenance of the Cottonwood Creek Trail. Recording the easement shall not be a condition to recordation of any final plat that does not include or directly affect the Cottonwood Creek Trail. Recording the mutually

Formatted: Font: 11 pt

Formatted: Font: 11 pt

acceptable Trail Easement is a material obligation under this Agreement and failure to record the Trail Easement as required under this Section 6.1 shall constitute a material default under this Agreement.

The construction of the Cottonwood Creek Trail and the grant of the permanent public-access easement constitute material public benefits supporting approval of the Conceptual Plan, the Rezone, the reduced commercial allocation, and this Agreement.

6.2 Maintenance of Cottonwood Creek Trail.

The Cottonwood Creek Trail, the trailhead, and the related trail improvements shall be owned, maintained, repaired, and replaced by one or more Owner Associations (defined below) in accordance with recorded CC&Rs, at no cost or expense to the County, while remaining open and accessible to the public. The public-access requirement for the Cottonwood Creek Trail is based, in part, upon the liability protections afforded to private property owners under Utah's Protection Statutes. In the event such statutory protections are repealed, materially limited, or judicially determined to be unavailable to Developer or the Owner Associations (defined below) for public use of the trail, Developer and/or the Owners Associations shall have the rights set forth in Section 5.1(d) of this Agreement.

6.3 Fire Department Dedication.

(a) **FD Parcel.** Developer shall dedicate and convey to the County, or its designated fire protection provider, the parcel identified as Parcel "FD" on the approved Conceptual Plan and depicted on **Exhibit G** (the "**FD Parcel**"). The FD Parcel shall contain not less than .18 acres (or approximately 8097 sq. ft) and shall be substantially consistent in location, dimensions, configuration, and area with **Exhibit G**. Before conveyance, Developer shall provide a record of survey and legal description prepared by a licensed professional land surveyor and subject to County approval. The FD Parcel shall have legally sufficient and practically usable access to a public roadway and reasonable access to utilities necessary for development and operation of a fire station. The parcel shall be suitable for its intended use, including construction, access, circulation, parking, and operation of a fire station, as reasonably determined by the County following review of applicable title, survey, environmental, geotechnical, access, and utility information.

~~(b)~~ The FD Parcel is located adjacent to the Commercial Parcel described in Section 4.7, as depicted on Exhibit B.

~~(b) **Timing of Conveyance.** Developer shall convey the FD Parcel in accordance with this Section 6.3 before recordation of the first final plat that includes or directly affects the FD Parcel. The conveyance shall not be a condition to the recordation of any earlier final plat that does not include or directly affect the FD Parcel.~~

(c) **Conveyance; Title.** The FD Parcel shall be conveyed to the County, Fire Department, or other County approved entity by Special Warranty Deed and in a condition sufficient to allow the FD Parcel to be lawfully and practically developed, accessed, operated, maintained, expanded, and continuously used as a fire station. Any title exceptions shall be subject to County's reasonable approval. Developer shall have no obligation to cure any title matter other than monetary liens required to be released at Closing and shall not be required to institute litigation, obtain third-party consents, acquire additional property interests, or incur costs to cure title. Developer shall not be required to provide title insurance. The FD Parcel identified in this Section 6.3 and depicted on Exhibit G shall be conveyed to the County in its then-existing, "AS IS, WHERE IS" condition, with all faults, without any representation or warranty by

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Developer concerning its physical condition, environmental condition, utility availability or capacity, suitability, or fitness for the County's intended use, except for any representation expressly stated in this Section 6.3. The County shall conduct such due diligence as it considers appropriate before accepting conveyance. Developer shall have no obligation to cure any deficiency; perform any investigation, remediation, grading, site preparation, or improvement; extend or provide utilities; or identify, acquire, dedicate, convey, or otherwise provide any substitute or alternative property. Developer's sole obligation shall be to convey the FD Parcel in accordance with the express conveyance requirements of this Section 6.3. The County shall not unreasonably withhold, condition, or delay its acceptance of the FD Parcel. Under no circumstances shall Developer be required to identify, acquire, dedicate, convey, or otherwise provide any substitute or alternative parcel.

(ed) **Public Benefit.** The dedication of the FD Parcel constitutes a material public benefit supporting approval of the Conceptual Plan, the Rezone, the reduced commercial allocation, and this Agreement

Formatted: Font: 11 pt, Not Bold

Formatted: Font: 11 pt

Formatted: Font: Bold

6.4 Tax Benefits.

The County acknowledges that Developer may seek tax benefits by reason of conveying and/or construction the Cottonwood Creek Trail and FD Parcel. Developer shall have sole responsibility to claim and qualify for any such tax benefits. The County shall reasonably cooperate, to the extent permitted by applicable law, in executing documents reasonably requested by the Developer to support any lawful application for such tax benefits, provided the County incurs no cost or liability in doing so.

7. CC&RS AND OWNER ASSOCIATION(S)

7.1 Establishment.

At the time of final plat review and approval, Developer shall record one or more declarations of conditions, covenants and restrictions regarding certain aspects of design and construction on the Property as amended from time to time ("CC&R's"). As more fully set forth in the CC&Rs, Developer shall create and establish one or more owner association(s) ("**Owner Associations**"), which shall be responsible for the implementation and enforcement of the CC&Rs, any building design standards, including but not limited to architectural reviews, open space, common areas, Cottonwood Creek Trail maintenance and private street maintenance. Recordation of the CC&Rs and creation of such Owner Associations shall be required at the time of final plat review and approval. County shall not be responsible for the implementation or enforcement of any such CC&Rs.

The Commercial Parcel described in Section 4.7 shall be excluded from the CC&Rs and from membership in each Owners Association, as provided in Section 4.7(g).

7.2 Amendment.

Except as provided in Section 7.4, the CC&Rs may be amended in accordance with the amendment procedures established in the CC&Rs and applicable law without County approval.

7.3 Association(s) Funding and Financial Requirements — Utah State Code Compliance.

Each Owners Association shall be organized, funded, and operated in compliance with the Utah Community Association Act, Utah Code Ann. §§ 57-8a-101 et seq.

7.4 CC&Rs Consistent with Agreement.

The CC&Rs and all other governing documents of each Owners Association shall remain consistent with this Agreement. No amendment to the CC&Rs or other governing documents may eliminate, reduce, impair, transfer, or otherwise modify any obligation imposed by this Agreement without the County's prior written approval.

8. VESTED RIGHTS AND LEGISLATIVE AUTHORITY

8.1 Vested Rights.

To the maximum extent permitted by applicable law, the Parties intend that this Agreement grants the Developer vested rights to develop the Property in accordance with the terms of this Agreement, the approved Conceptual Plan, the Rezone, and the approvals granted hereunder. Except as expressly provided in this Agreement or otherwise required by applicable law, the County shall not modify or impair those vested rights. The Parties intend that the rights granted by this Agreement constitute vested land use rights under Utah Code § 17-79-803 and applicable Utah common law. Such vested rights shall be governed by the land use ordinances, regulations, and other applicable laws in effect on the Effective Date, except as otherwise provided herein or required by applicable law.

8.2 Reserved Legislative and Police Powers.

Nothing in this Agreement limits, waives, delegates, or contracts away the County's legislative, governmental, regulatory, administrative, enforcement, emergency, or police powers. The County retains all authority conferred by applicable law to protect the public health, safety, and welfare and to adopt, interpret, administer, and enforce generally applicable laws and regulations, subject only to vested rights expressly established by this Agreement and applicable law. No provision of this Agreement shall be construed to prevent the County from taking any action authorized or required by law in response to an emergency, unlawful conduct, a threat to public health or safety, or a compelling countervailing public interest.

9. FURTHER APPROVALS

9.1 Subdivision, Plat Approval, and Compliance with Design Conditions.

Developer expressly acknowledges and agrees that nothing in this Agreement will be deemed to relieve it from the obligation to comply with all applicable requirements necessary for approval and recordation of final plat(s) as set forth herein and in the Land Use Code.

9.2 Timeliness.

Where further approvals by the County are required under this Agreement or applicable law, the Parties shall cooperate in good faith to facilitate the timely processing of applications. The County shall process complete applications in accordance with the procedures and timeframes established by the County Code and applicable law, and the Developer shall timely provide all information reasonably required to process such applications.

10. PUBLIC IMPROVEMENTS, SUBDIVISION PHASING, AND WARRANTY

10.1 Construction of Public Improvements.

All public improvements located within the Property and Project will be constructed and installed at the Developer's sole expense in accordance with applicable final plat(s) (including the approved construction drawings and specifications), this Agreement, and applicable law.

10.2 Inspection and Acceptance.

Upon completion of the applicable public improvements, Developer may submit a written request for inspection accompanied by certification from Developer's engineer that the improvements have been completed in accordance with the approved plans and specifications, this Agreement, applicable County standards, and applicable law. Developer shall also provide all required testing results, certifications, record drawings, operation and maintenance documents, and other information reasonably required for inspection and acceptance.

The County shall inspect the improvements and provide Developer with written notice identifying any incomplete, defective, or noncompliant work within a reasonable period consistent with applicable law. Developer shall correct all identified deficiencies and request reinspection. The County may conduct additional inspections and require additional testing reasonably necessary to verify compliance.

The County shall accept the public improvements only after determining that they have been completed in compliance with the approved plans and specifications, this Agreement, applicable County standards, and applicable law and after Developer has provided all required documentation, paid applicable fees, corrected identified deficiencies, and completed any required dedication or conveyance.

Any inspection or acceptance period shall be reasonably extended for incomplete submissions, required testing, correction or reinspection of deficient work, inclement weather, emergencies, unavailability of necessary personnel or consultants, or other circumstances beyond the County's reasonable control. County inspection or acceptance shall not waive latent defects, defective workmanship or materials, fraud, applicable warranty obligations, or conditions that could not reasonably have been discovered during inspection.

10.3 Improvement Completion Assurance.

Prior to recordation of a final plat for any phase, Developer shall enter into an improvement completion agreement and provide improvement completion assurance and warranty assurance in accordance with applicable state law and the applicable provisions of the County Code, including § 155.420. The assurances shall cover all improvements required to be included and shall be provided, administered, reduced, released, replaced, and enforced in accordance with applicable state law and the applicable provisions of the County Code.

10.4 Roadways.

Private roads shall be designed and constructed per County standards and cross-sections as shown on **Exhibit CP** attached hereto. The County is not responsible for maintenance of private roads. All private roads within the Project shall remain privately owned and shall be operated, maintained, repaired, and replaced by one or more Owner Associations at no cost or expense to the County. The Commercial Parcel described in Section 4.7 takes direct access from Old Highway Road, does not use the private roadways within the Project, and is not subject to any obligation with respect to the ownership or maintenance of such private roadways.

10.5 Utilities.

Developer shall design, construct, and install all sewer, culinary water, secondary (irrigation) water, stormwater, and other utility infrastructure required to serve the Project in accordance with the approved construction plans, this Agreement, the requirements of the applicable utility providers, and applicable County standards. All utility improvements shall be subject to inspection and acceptance by the applicable utility provider and, where applicable, the County.

10.6 Subdivision Phasing.

The County acknowledges that the Project is anticipated to be developed in multiple phases, with sequencing subject to market conditions, infrastructure installation, and County approvals. The Developer may submit multiple preliminary and final plat applications from time to time to develop and/or construct portions of the Project in phases consistent with Chapter 155.415–424 of the County Code and Utah Code Ann. §17-79-704. The following phasing standards shall apply:

(a) **Phase Submittals.** Each phase shall be submitted as a separate preliminary and final plat application identifying the lots, common areas, public improvements, and amenities proposed within that phase.

(b) **Infrastructure Sequencing.** Public infrastructure required for each phase shall be constructed and completed in accordance with approved construction drawings and County standards prior to issuance of building permits or certificates of occupancy for that phase.

(c) **Completion Assurance Per Phase.** The Developer shall provide completion assurance in an amount equal to one hundred ten percent (110%) of the engineer-approved cost of all required public improvements not yet installed at the time of plat recordation for each respective phase.

(d) **Amenity Phasing.** Project Amenities shall be phased and completed in accordance with the schedule set forth in Section 5.2.

(e) **Phase Independence.** Each final plat phase shall be capable of standing alone as a functional subdivision with adequate access, utilities, and required improvements, without dependency on improvements in a future phase, unless otherwise approved in writing by the County.

(f) **Phase Modifications.** Minor modifications to phasing boundaries or sequencing that remain substantially consistent with the approved Conceptual Plan may be approved administratively by the County. Material modifications shall require amendment of this Agreement or such additional approvals as required by the County Code.

(g) **Commercial Parcel Phasing.** The Commercial Parcel shall be created as a separate legal lot by recorded final plat, and the pad-ready improvements described in Section 4.7(c) shall be constructed, not later than recordation of the final plat for the second residential phase of the Project. Developer may include the Commercial Parcel within an earlier final plat at Developer's election.

10.7 Improvement Warranty for Subdivisions — Utah State Code Compliance.

Upon the County's initial acceptance of the public improvements, and in compliance with Utah Code Ann. §17-79-707 and applicable County Code standards, the Developer shall provide the following warranty assurances:

(a) **Warranty of Improvements.** Developer warrants that all public improvements installed within the subdivision are constructed in accordance with the approved plans and specifications, are free from defects in materials and workmanship ("**Improvement Warranty**"), and will remain in satisfactory condition for a period of one (1) year from the date of the County's written acceptance (the "**Warranty Period**"), consistent with the minimum warranty requirement under Utah Code Ann. §17-79-707.

(b) **Defect Notification and Cure.** If the County identifies a material defect during the Warranty Period, the County shall provide Developer with written notice describing the nature and location of the defect and specifying a reasonable period for Developer to commence corrective work based upon the nature, severity, and urgency of the defect. Developer shall commence corrective work within the time specified in the notice and shall thereafter diligently prosecute the work to completion. Notwithstanding the foregoing, if the County reasonably determines that a defect constitutes an imminent threat to public health, safety, or property requiring immediate action, the County may require Developer to respond immediately or within such shorter period as is reasonable under the circumstances. If Developer fails to timely commence or diligently pursue the required corrective work, or fails to respond to an emergency condition within the time reasonably specified by the County, the County may perform or cause the corrective work to be performed and recover its reasonable, documented costs from the warranty security to the extent such costs are attributable to Developer's warranty obligations.

(c) **Release of Warranty Security.** Upon expiration of the Warranty Period and written confirmation by the County Engineer that all identified defects have been corrected, the County shall release the warranty security to Developer within the period required by Utah Code Ann. §17-79-707. ~~thirty (30) days.~~ The County shall not unreasonably withhold or delay such release.

(d) **Third-Party Beneficiaries.** No lot purchaser or other third party shall have rights as a third-party beneficiary under the Improvement Warranty or warranty security. All warranty obligations run solely between Developer and the County.

11. TERM AND MISCELLANEOUS PROVISIONS

11.1 Term.

This Agreement shall remain in effect for fifteen (15) years from the Effective Date unless terminated or amended in writing. The term may be extended by mutual written agreement of the Parties, subject to approval by the Morgan County Commission. Expiration or termination of this Agreement shall not release or extinguish any obligation, liability, default, enforcement right, or remedy that accrued before expiration or termination. All obligations intended by their nature or express terms to continue, including obligations concerning public access, ownership and maintenance of private infrastructure and Project Amenities, Owners Association funding and reserves, land dedications, recorded easements and restrictions, warranties, indemnification, and enforcement of completed or continuing obligations, shall survive expiration or termination and remain binding upon the applicable parties and their successors and assigns.

11.2 County Fees.

Developer acknowledges that County fees may increase in accordance with applicable law.

11.3 Construction Standards.

Construction standards for all portions of the development of the infrastructure for the Property will be governed by the most current edition of the County Code, the Utah State Building, Plumbing, Mechanical, Electrical Codes, current engineering standards and the International Building Code as enforced by the County as the primary governing agency, at the time of application for building permit. No part of this Agreement will be deemed to supersede these standards. Developer will be required to comply with all conditions necessary for the issuance of a building permit, including, without limitation, any bonding or guaranty requirements generally applied by the County.

11.4 Dedication of Public Infrastructure.

Developer shall dedicate or convey to the County only those roadways, rights-of-way, and other public infrastructure expressly required by this Agreement, an approved final plat, or applicable law and expressly accepted by the County. Each conveyance shall be by plat dedication, special warranty deed, or other instrument acceptable to the County, at no cost to the County and free of all liens, encumbrances, interests, and title exceptions except those expressly approved in writing by the Parties.

Public access shall not constitute or imply dedication or County acceptance of any privately owned property or improvement. Unless otherwise provided in a separate written agreement approved by the Morgan County Commission, all Project Amenities, parks, trails, trailheads, public-access easements, public parking areas, common-area sidewalks, landscaping, private roadways, and privately owned stormwater facilities shall remain privately owned and shall be operated, maintained, repaired, replaced, and, where applicable, cleared of snow by one or more Owner Associations at no cost to the County.

The County shall assume ownership or maintenance responsibility only for public roadways and other public infrastructure expressly accepted into the applicable County system following completion, inspection, and acceptance in accordance with this Agreement and applicable law. Public use or access, standing alone, shall not obligate the County to own, operate, maintain, repair, or replace any property or improvement.

11.5 Final Plat Amendments.

In the event Developer desires to make minor changes to any respective final plat(s) before they are recorded, Developer will submit such changes to County staff for approval. So long as such changes are consistent with this Agreement and applicable law, County staff will approve such changes. If County staff determines that such changes are inconsistent with the provisions of this Agreement, Developer must seek approval from the County Planning Commission and the County Commission.

12. ASSIGNMENT

12.1 Binding on Successors and Assigns.

This Agreement shall be binding upon and inure to the benefit of the Parties and their respective permitted successors and assigns.

12.2 Assignment by Developer.

Developer may assign this Agreement only with prior written County consent, which consent shall not be unreasonably withheld, conditioned, or delayed. An assignee must demonstrate capability to perform the obligations assumed. Developer shall remain liable under this Agreement unless expressly released in writing by the County.

12.3 Non-Assignment.

Lot sales and mortgages in the ordinary course of business do not constitute an assignment requiring County consent.

12.4 Obligations of Assignee.

Assignees shall assume all Developer's obligations under this Agreement and shall be substituted accordingly. Developer shall remain liable unless released by the County in writing.

13. GENERAL TERMS

13.1 Agreement to Run with the Land.

This Agreement shall be recorded in the Office of the Morgan County Recorder, shall be deemed to run with the Property, and shall encumber the same; and shall be binding on and inure to the benefit of all successors and assigns of Developer in the ownership or development of any portion of the Property.

13.2 Severability.

In the event any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall remain valid and binding upon the Parties. One or more waivers of any term, condition, or other provision by either Party shall not be construed as a waiver of a subsequent breach of the same or any other provision.

13.3 No Third-Party Beneficiary.

The provisions of this Agreement are and will be for the benefit of Developer and the County only and are not for the benefit of any third person or entity.

13.4 Choice of Law and Venue.

Any dispute regarding this Agreement shall be heard and settled under the laws of the State of Utah. Any Utah litigation regarding this Agreement shall be filed in the ~~Third~~Second District Court for Morgan County, Utah. Any federal litigation shall be filed in the United States District Court for the District of Utah.

13.5 Entire Agreement.

This Agreement contains the entire agreement between the Parties with respect to the subject matter hereof and integrates all prior conversations, discussions, or understandings of whatever kind or nature, and may only be modified by a subsequent writing duly executed and approved by the Parties.

13.6 Notice.

All notices required or permitted under this Agreement shall be given in writing and delivered by: (a) personal delivery; (b) certified mail, return receipt requested; (c) electronic delivery; or (d) a nationally recognized overnight courier service, addressed as follows:

Developer:

BCP Development, LLC
Attn: Peter Evans
300 S 1350 E St. 2nd Floor
Lehi, UT 84043
Email: pete@flagshiphomes.com

County:

Morgan County
Attn: County Attorney
48 W Young St, PO Box 886
Morgan, UT 84050-9000
Email: _____
Copy to:

Morgan County Clerk

48 W Young St,
PO Box 886
Morgan, UT 84050-9000
Email: _____

13.6.1 Effective Notice.

Except as otherwise provided in this Agreement, each Notice shall be effective and deemed delivered on the earlier of: (a) Physical Delivery — its actual receipt if delivered personally or by courier; (b) Electronic Delivery — its actual receipt if delivered by email; or (c) Mail Delivery — on the day the Notice is postmarked, postage prepaid, by First Class or Certified United States Mail.

13.6.2 Change of Notice Address.

Any Party may change its address for Notice under this Agreement by giving written Notice to the other Party in accordance with the provisions of this Section.

13.7 Default and Dispute Resolution.

If either Party materially fails to perform an obligation under this Agreement, the non-defaulting Party may provide written notice specifying: (i) the claimed event of default; (ii) the provisions ~~written~~ claimed to be in default; and (iii) why the default is claimed to be material. Unless a different period is required by applicable law or the County Code, the defaulting Party shall have thirty (30) days after receipt of notice to cure the default or, if the default cannot reasonably be cured within thirty (30) days, to commence and diligently pursue the cure to completion.

The notice-and-cure and dispute-resolution procedures in this Section apply only to contractual remedies arising under this Agreement. They do not limit, delay, modify, or replace the County's legislative, regulatory, administrative, enforcement, emergency, or police powers; the enforcement procedures or remedies available under applicable law or the County Code; or the County's authority to address

unlawful work, threats to public health or safety, deficient or expiring financial security, or violations of permits, plats, conditions of approval, or other development requirements.

During an uncured default, the County may exercise all remedies authorized by this Agreement, applicable law, and the County Code, including withholding, denying, suspending, conditioning, or revoking permits, certificates of occupancy, inspections, final plat approvals, future phase approvals, and other development approvals. The County's exercise of those remedies is not conditioned upon completion of the meet-and-confer or mediation procedures below.

(a) **Voluntary Resolution.** Without limiting or delaying the County's enforcement authority, the Parties shall meet within twenty-one (21) calendar days after notice of a contractual default and make a good-faith effort to resolve the matter.

(b) **Meet and Confer.** If any Party gives notice of a default, the Parties shall meet within twenty-one (21) calendar days of the notice and make good faith effort to resolve the issues specified in the notice.

(c) **Mediation.** If the Parties are unable to resolve the notice of default after the Meet and Confer, the Parties shall attempt within fifteen (15) calendar days to appoint a mutually acceptable mediator. If the Parties cannot agree on a single mediator, each shall appoint their own representative who shall together choose the mediator. The Parties shall split mediator fees equally. The chosen mediator shall within fifteen (15) calendar days, review the positions of the Parties regarding the dispute and promptly attempt to mediate the issue between the Parties. If the Parties are unable to reach agreement on the notice of default, the mediator shall notify the Parties in writing of the resolution that the mediator deems appropriate. The mediator's opinion shall not be binding on the Parties.

(d) **Remedies.** If the Parties are not able to resolve the default by mediation, the Parties shall have all rights and remedies available at law and in equity, including but not limited to injunctive relief, specific performance, and/or damages.

13.8 Force Majeure.

A Party's time to perform an obligation under this Agreement may be reasonably extended when performance is actually prevented by an unforeseeable event beyond that Party's reasonable control, including natural disasters, declared emergencies, war, civil disturbance, governmental restrictions, or judicial orders not resulting from that Party's act, omission, or violation of law. Ordinary weather conditions, changes in market conditions, financing difficulties, increased costs, or reasonably foreseeable shortages of labor or materials do not constitute force majeure.

The affected Party shall provide written notice describing the event and its anticipated effect on performance within ten (10) days after becoming aware of the event and shall diligently mitigate the delay and resume performance as soon as reasonably practicable. Any extension shall be limited to the period during which performance is actually prevented. Force majeure does not excuse payment obligations, eliminate any obligation, authorize occupancy or development beyond an applicable completion threshold, or prevent the County from taking action necessary to protect public health or safety.

13.9 Attorney's Fees.

The prevailing Party in any enforcement action shall be entitled to recover its reasonable attorneys' fees and costs incurred in such action, including any appeal.

13.10 No Waiver.

A Party's failure to enforce a right shall not constitute a waiver of any rights. Any waiver must be in writing and signed by the waiving Party to be effective.

13.11 Amendment.

This Agreement may be amended in whole or in part by the mutual written consent of the Parties or by their successors-in-interest or assigns. Any such amendment shall be recorded in the official records of the Morgan County Recorder's Office. No oral modifications shall be valid or enforceable.

13.12 Mutual Drafting.

Each Party has participated in negotiating and drafting this Agreement, and therefore no provision of this Agreement shall be construed for or against either Party based on which Party drafted any particular portion.

13.13 Further Actions and Instruments.

The Parties agree to provide reasonable assistance to the other and cooperate to carry out the intent and fulfill the provisions of this Agreement. Each of the Parties shall promptly execute and deliver all documents and perform all acts as necessary to carry out the matters contemplated by this Agreement.

[Signatures appear on the following page]

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by and through their respective, duly authorized representatives as of the day and year first herein above written.

DEVELOPER: BCP Development, LLC

By: _____

Name: Peter Evans

Title: Manager

STATE OF UTAH)

:ss

COUNTY OF _____)

The foregoing instrument was acknowledged before me this ____ day of _____, 2026, by _____.

Notary Public

Residing at: _____

My Commission Expires: _____

COUNTY: Morgan County

By: _____

Name: _____

Title: _____

STATE OF UTAH)

:ss

COUNTY OF _____)

The foregoing instrument was acknowledged before me this ____ day of _____, 2026, by _____.

Notary Public

Residing at: _____

My Commission Expires: _____

EXHIBIT A

Legal Description of the Property

A parcel of land located in all Section 25, Township 05 North, Range 01 East, Salt Lake Base and Meridian, located in Morgan County, Utah, being more particularly described as follows:

Beginning at a point N89°38'55"E 1331.96 feet along the Quarter Section line from the West Quarter Corner of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian; running thence along said quarter Section Line N 89°38'55" E 1,320.26 feet; thence along the northerly line of Cottonwood Creek N 73°05'20" E 119.65 feet to the westerly right-of-way line of Old Highway Road; thence along said right-of-way line S 47°29'33" E 71.21 feet; thence S 76°00'00" W 176.10 feet; thence South 161.30 feet; thence S 75°40'00" E 167.73 feet; thence S 25°59'18" W 32.12 feet; thence S 62°36'30" E 198.05 feet; thence N 35°55'46" E 190.17 feet to the southerly right-of-way line of Old Highway Road; thence along said right of way line the following two (2) courses: (1) Southeasterly along the arc of a non-tangent curve to the left having a radius of 995.40 feet a distance of 184.74 feet through a central angle of 10°38'02" Chord: S 65°22'26" E 184.48 feet; (2) thence S 70°40'00" E 1,022.71 feet to the westerly line of that Warranty Deed recorded February 25, 2004 as Entry No. 095215 in the Morgan County Recorder's Office; thence along said Warranty Deed S 30°27'00" W 715.74 feet; thence N 63°40'00" W 467.79 feet; thence N 47°46'00" W 231.80 feet; thence N 82°00'00" W 225.00 feet; thence S 60°31'29" W 203.90 feet; thence S 69°02'00" W 216.83 feet to the easterly line of Parcel 1 described in the Special Warranty Deed recorded January 05, 2018 as Entry No. 143682 in the Morgan County Recorder's Office; thence along said easterly line of parcel 1 N 00°11'13" E 327.26 feet; thence West 1,330.72 feet to the easterly line of Parcel 2 in the aforementioned Special Warranty deed; thence along said easterly line of Parcel 2 line N 00°05'24" E 705.14 feet to the point of beginning.

Containing 43.15 acres, more or less.

EXHIBIT B
Conceptual Plan and Narrative

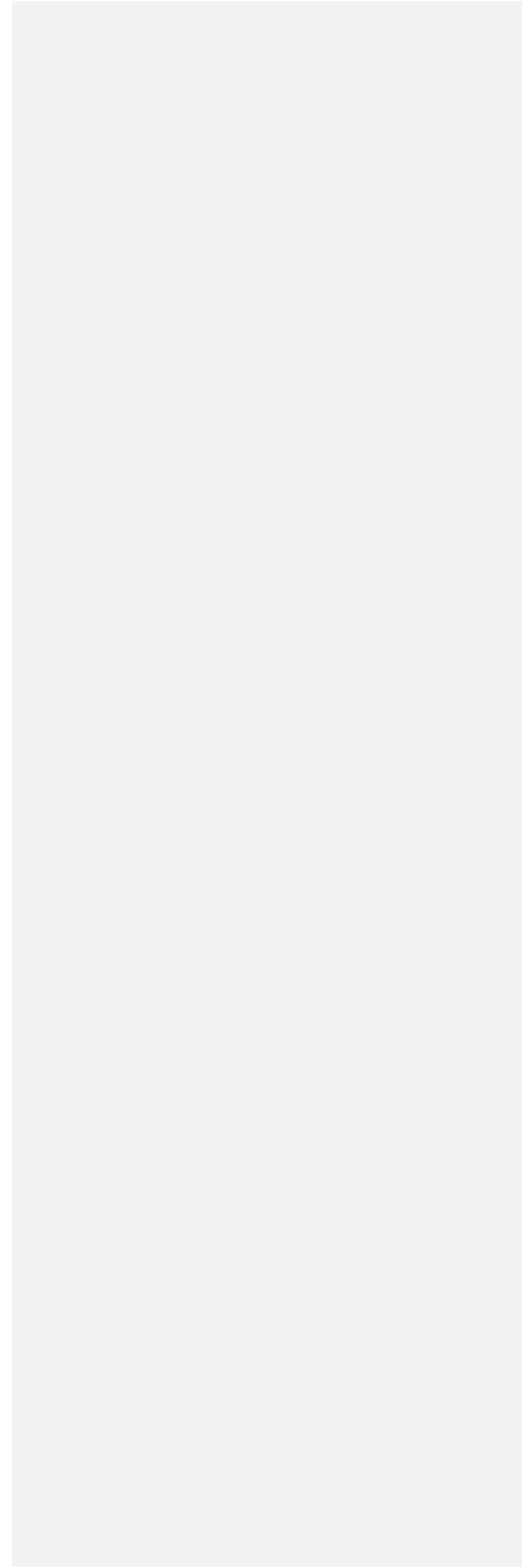


EXHIBIT C
Public and Private Road Cross-Section Standards

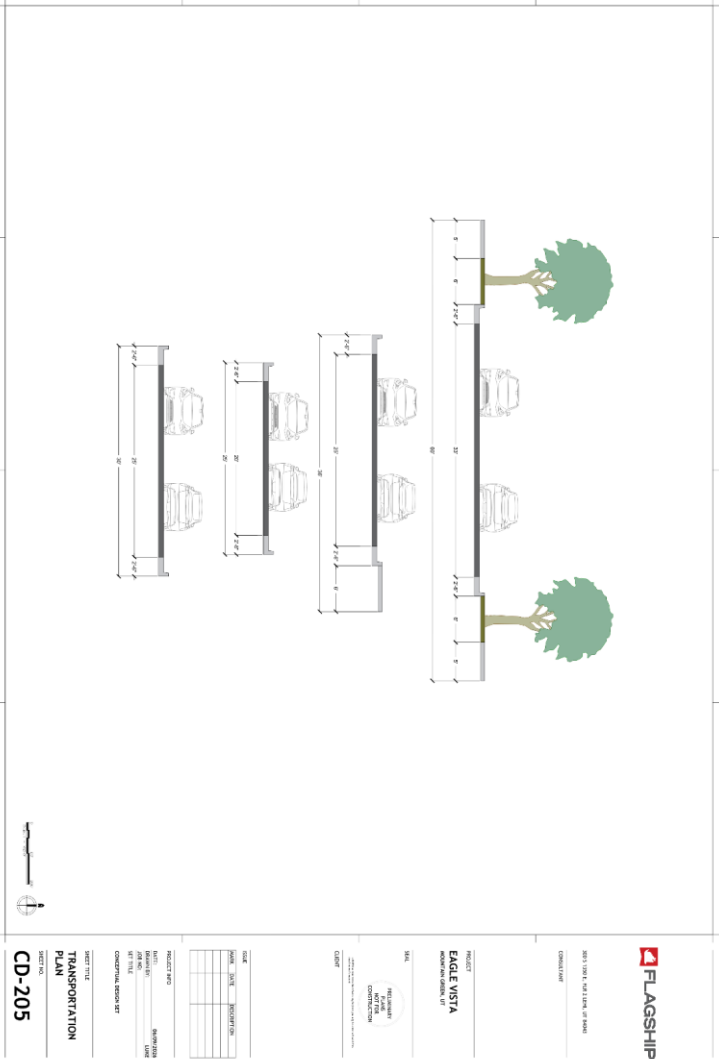
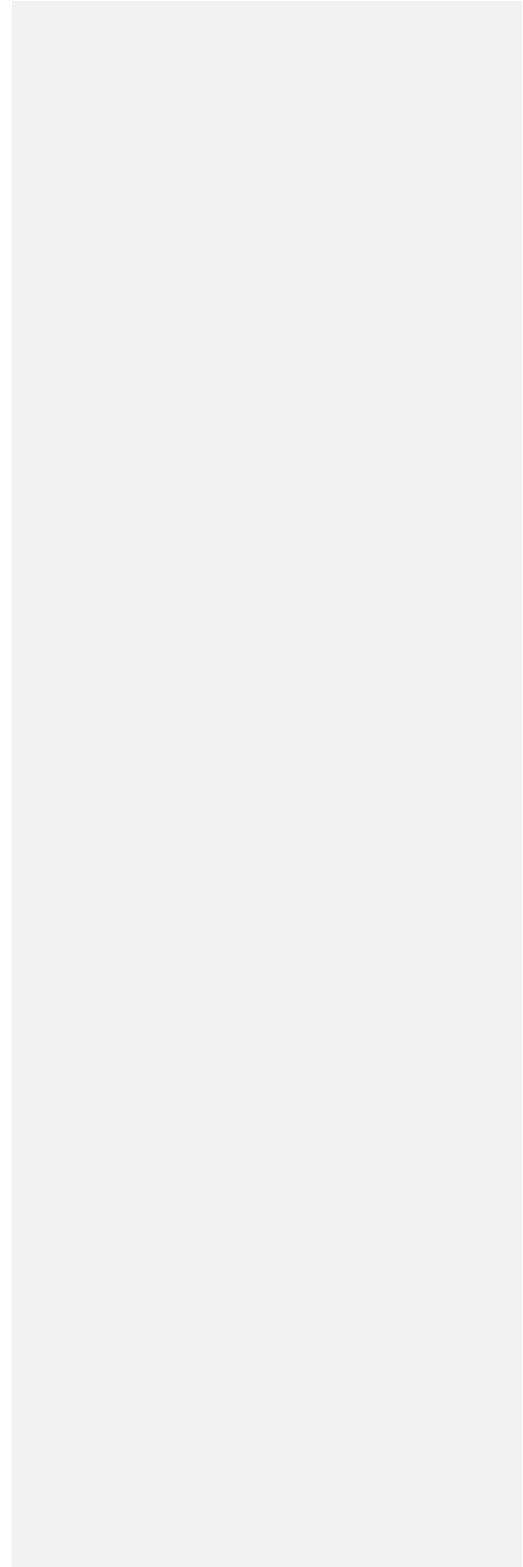
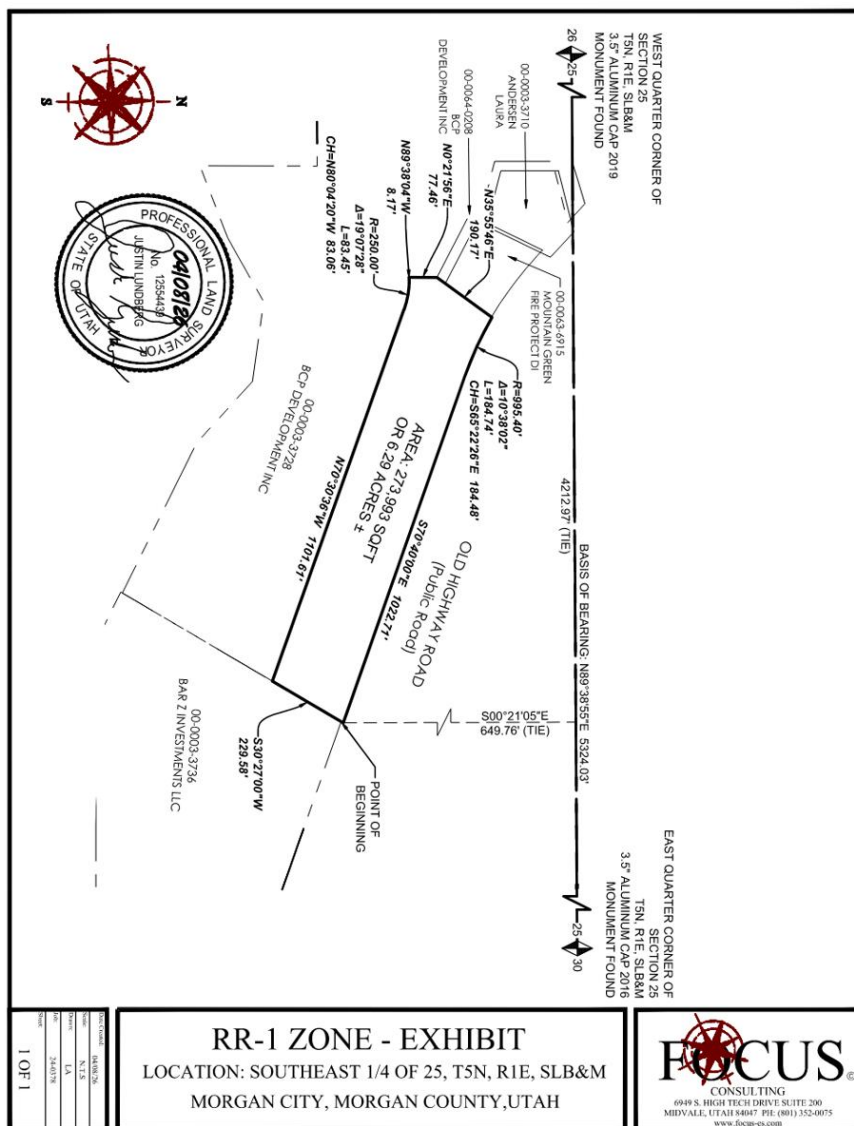


EXHIBIT D
Rezone Area Description and Depiction







**LEGAL DESCRIPTION
PREPARED FOR
BCP DEVELOPMENT INC
MORGAN CITY, UTAH**

April 7, 2026
24-0378
LA

RR-1 ZONE - LEGAL DESCRIPTION

A part of the Southeast Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian, located in Morgan City, Morgan County, Utah, being more particularly described as follows:

Beginning on the Southerly right-of-way line of Old Highway Road, said point also being located N89°38'55"E 4212.97 feet along the Quarter Section line and S0°21'05"E 649.76 feet from the West Quarter Corner of Section 25, Township 5 North, Range 1 East, Salt Lake Base and Meridian; running thence S30°27'00"W 229.58 feet; thence N70°30'36"W 1,101.61 feet; thence along the arc of a curve to the left with a radius of 250.00 feet a distance of 83.45 feet through a central angle of 19°07'28" Chord: N80°04'20"W 83.06 feet; thence N89°38'04"W 8.17 feet; thence N00°21'56"E 77.46 feet to the Southerly right-of-way of the Old Highway Road; thence along said right-of-way line the following two (2) courses: (1) N35°55'46"E 190.17 feet; (2) thence Southeasterly along the arc of a non-tangent curve to the left having a radius of 995.40 feet (radius bears: N29°56'34"E) a distance of 184.74 feet through a central angle of 10°38'02" Chord: S65°22'26"E 184.48 feet; thence S70°40'00"E 1,022.71 feet to the point of beginning.

Containing 273,993 square feet or 6.29 acres, more or less.

Exhibit E (Reserved)

Exhibit F
Cottonwood Creek Trail Alignment and Trailhead

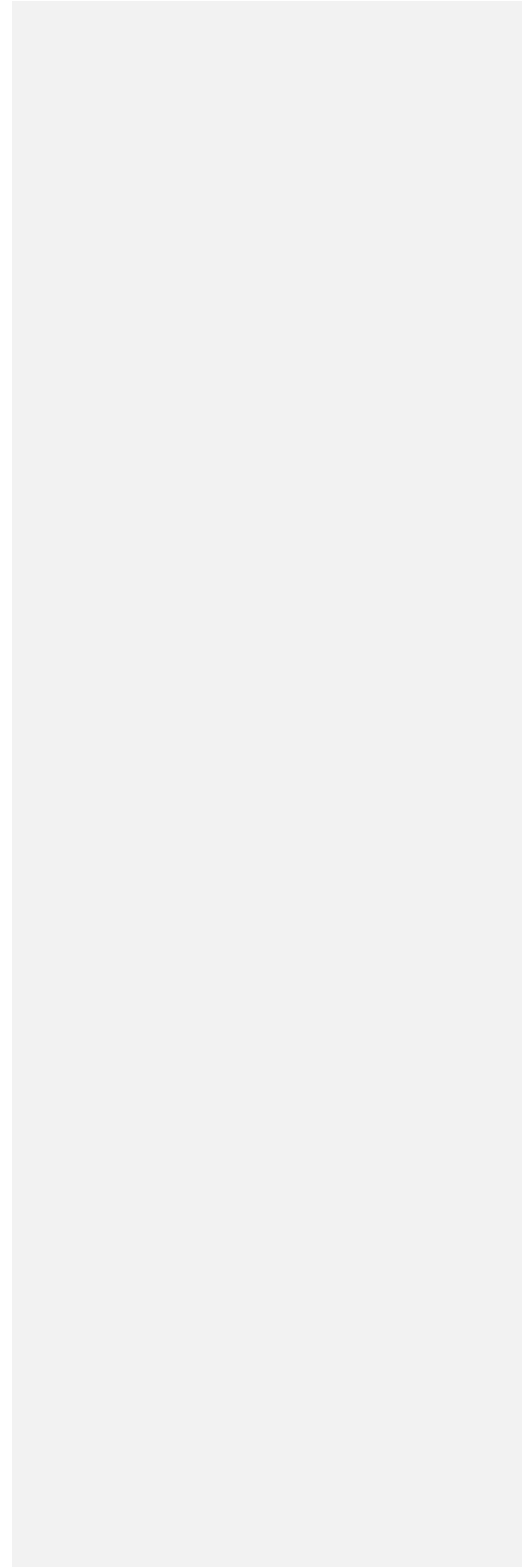
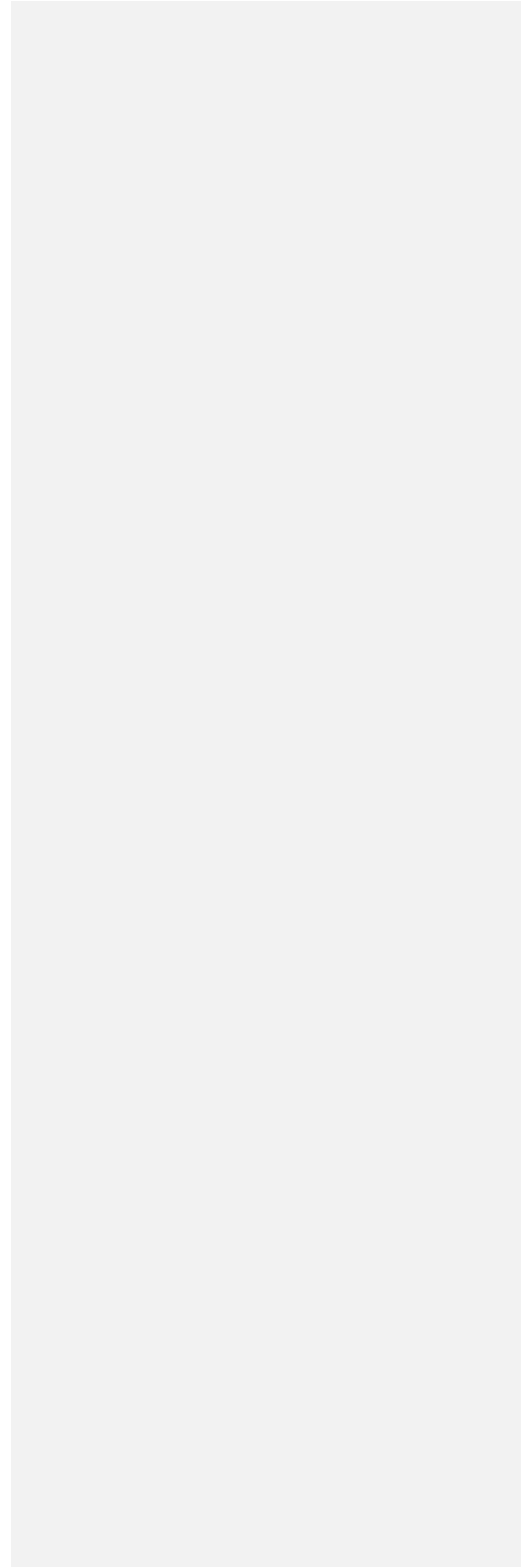


EXHIBIT G
Fire Department Parcel ("FD Parcel")





Contract # _____

STATE OF UTAH CONTRACT

1. **CONTRACTING PARTIES:** This agreement is between the State of Utah, Division of Technology Services, Utah Geospatial Resource Center (UGRC), Taylorsville State Office Building, 4th Floor, 4315 S. 2700 W, Taylorsville, UT 84129, (Agency Code 110) referred to as STATE, and the following County, which is a Government Agency.

County Name: Morgan County

Address: 48 W Young St. Rm. 21

City, State, Zip: Morgan, UT 84050

Federal ID# _____ Vendor Code _____ Commodity Code _____

2. **GENERAL PURPOSE OF CONTRACT:** The general purpose of this contract is for the County to receive Monument Replacement and Restoration Committee (MRRC) funding as outlined in the 2015 Senate Bill 264 for monument replacement, preservation and restoration of Public Land Survey System section corners.
3. **CONTRACT PERIOD:** Effective date 7/1/2026. Termination date 6/30/2027, unless terminated early or extended in accordance with the terms and conditions of this contract. The MRRC may conduct a mid-term contract review to assure the work is being done or scheduled for completion within the terms of this contract. If progress toward completion of the work cannot be documented, the COUNTY risks the possibility of contract termination. The deliverable for this contract is due May 15, 2027.
4. **GRANT VALUE:** County will be paid a maximum of \$24,836.80 for funds authorized by this contract.
5. **ATTACHMENTS INCLUDED AS PART OF THIS CONTRACT:**
Attachment A: Standard Terms and Conditions
Attachment B: Scope of Work
Attachment C: Field Procedures
Attachment D: Deliverables
Any conflicts between Attachment A and other Attachments will be resolved in favor of Attachment A.
6. **DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED HERETO:**
A. All other governmental laws, regulations, or actions applicable to goods and/or services authorized by this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

COUNTY

STATE

Signature

Date

Name and Title of Signer (Type or Print)

Sean A. Fernandez, Cadastral Manager
Utah Geospatial Resource Center (UGRC)

Division of Technology Services

Division of Finance



County Commission Agenda Request Form

All Agenda items, including back-up materials, must be submitted to:

Morgan County
Attn: Kate Becker
48 West Young Street
P O Box 886
Morgan, UT 84050
Phone: 435.800.8724

****ALL DOCUMENTATION IS DUE ON OR BEFORE 12:00 PM ON THE TUESDAY PRIOR TO A SCHEDULED COUNTY commission MEETING****

Email: kbecker@morgancountyutah.gov

This form must be submitted, along with any required documentation, or the Agenda Item will not be scheduled until the next County commission Meeting

commission Meeting Date: 08/18/2026 Time Requested: _____
Name: Garrett Smith Phone: (801) 845-4006
Address: 48 West Young Street
Email: gsmith@morgancountyutah.gov Fax: _____
Associated County Department: Morgan County Attorney's Office

PURPOSE FOR THE AGENDA ITEM - MUST BE SPECIFIC:

Request for a budget transfer to cover temp legal costs as we navigate a deputy attorney vacancy. Further explanation is included in the attached document.

WILL YOUR AGENDA ITEM BE FOR:

DISCUSSION
DECISION
BOTH
INFORMATION ONLY

☐
☐
☒
☐



2026 BUDGET CHANGE REQUEST

Date 8/11/26

Department Morgan County Attorney's Office

Department Head Signature *Garrett J. Smith*

Amount \$25,000

Move from GL Account# 10-4145-110

Move to GL Account # 10-4145-370

Brief Description

Our deputy attorney resigned in March, so we have had to rely on Dean
Saunders to cover Justice Court completely since that time. I have also brought
on an intern with a year of law school under her belt to fill in the gaps of losing
our deputy attorney. Both are doing great work! We will still have a surplus in
Permanent Employees (10-4145-110) and Employee Benefits (10-4145-130) at
the end of the year. I have borrowed from other GLs as a stop gap.

Clerk/Auditor Use Only

Date Entered



County Commission Agenda Request Form

All Agenda items, including back-up materials, must be submitted to:

Morgan County
Attn: Kate Becker
48 West Young Street
P O Box 886
Morgan, UT 84050
Phone: 435.800.8724

****ALL DOCUMENTATION IS DUE ON OR BEFORE 12:00 PM ON THE TUESDAY PRIOR TO A SCHEDULED COUNTY commission MEETING****

Email: kbecker@morgancountyutah.gov

This form must be submitted, along with any required documentation, or the Agenda Item will not be scheduled until the next County commission Meeting

commission Meeting Date: 08/18/2026 Time Requested: _____
Name: Garrett Smith Phone: (801) 845-4006
Address: 48 West Young Street
Email: gsmith@morgancountyutah.gov Fax: _____
Associated County Department: Morgan County Attorney's Office

PURPOSE FOR THE AGENDA ITEM - MUST BE SPECIFIC:

Craig Ide with the State with UDOT Division of Aeronautics is requesting the County sign the State Contract for the Morgan County Airport Pavement Preservation Project. Seeking review and approval of the Grant Agreement terms.

WILL YOUR AGENDA ITEM BE FOR:

DISCUSSION
DECISION
BOTH
INFORMATION ONLY

☐
☐
☒
☐

FI 85
08/2005
Division of Finance



This cover sheet is to be used if
you are not using the Standard
Contract Agreement FI 84.

Contract # _____
Assigned by the Division of Finance

STATE OF UTAH CONTRACT COVER SHEET

This contract is entered into as a result of:

- ☐ The procurement process on bid # _____
- ☐ The procurement process on requisition # _____ FY _____
YYY
- ☐ Pre-approved sole source (approval attached)
- ☒ Agency grant, land purchase, DAS-Purchasing delegation
- ☐ Contract with other state agency or political subdivision
- ☐ Under \$2,000 (total amount per fiscal year)
- ☐ Agency exemption from DAS-Purchasing approval
- ☐ Revenue agreement

1. Agency Name: 810 - Dept. of Transportation
Division: Aeronautical Operations

2. General Purpose of Contract:

Project Application & Grant Agreement for State Aid for Development of Public Airports for
FY2026 "Pavement Preservation" project at the Morgan County.

3. Contractor Name: Morgan County

4. Contract Period: Effective Date: 5/29/2026
MM/DD/YYYY

Termination Date: 12/31/2027
MM/DD/YYYY

5. Authorized Amount: \$103,765.00

6. Vendor #: 50534G

7. Commodity Code(s): 99999

Agency contact for questions during the contract approval process.

Craig Ide
Agency Contact

(801) 209-6772
Phone Number

ATTACHMENT A: STATE OF UTAH STANDARD TERMS AND CONDITIONS

1. **AUTHORITY:** Provisions of this contract are pursuant to the authority set forth in 63-56, Utah Code Annotated, 1953, as amended, Utah State Procurement Rules (Utah Administrative Code Section R33), and related statutes which permit the State to purchase certain specified services, and other approved purchases for the State.
2. **CONTRACT JURISDICTION, CHOICE OF LAW, AND VENUE:** The provisions of this contract shall be governed by the laws of the State of Utah. The parties will submit to the jurisdiction of the courts of the State of Utah for any dispute arising out of this Contract or the breach thereof. Venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County.
3. **LAWS AND REGULATIONS:** Any and all supplies, services and equipment furnished will comply fully with all applicable Federal and State laws and regulations.
4. **RECORDS ADMINISTRATION:** The Contractor shall maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the Contractor for costs authorized by this contract. These records shall be retained by the Contractor for at least four years after the contract terminates, or until all audits initiated within the four years, have been completed, whichever is later. The Contractor agrees to allow State and Federal auditors, and State Agency Staff, access to all the records to this contract, for audit and inspection, and monitoring of services. Such access will be during normal business hours, or by appointment.
5. **CONFLICT OF INTEREST:** Contractor represents that none of its officers or employees are officers or employees of the State of Utah, unless disclosure has been made in accordance with 67-16-8, Utah Code Annotated, 1953, as amended.
6. **CONTRACTOR, AN INDEPENDENT CONTRACTOR:** The Contractor shall be an independent contractor, and as such, shall have no authorization, express or implied, to bind the State to any agreements, settlements, liability, or understanding whatsoever, and agrees not to perform any acts as agent for the State, except as herein expressly set forth. Compensation stated herein shall be the total amount payable to the Contractor by the State. The Contractor shall be responsible for the payment of all income tax and social security amounts due as a result of payments received from the State for these contract services. Persons employed by the State and acting under the direction of the State shall not be deemed to be employees or agents of the Contractor.
7. **INDEMNITY CLAUSE:** The Contractor agrees to indemnify, save harmless, and release the State OF UTAH, and all its officers, agents, volunteers, and employees from and against any and all loss, damages, injury, liability, suits, and proceedings arising out of the performance of this contract which are caused in whole or in part by the negligence of the Contractor's officers, agents, volunteers, or employees, but not for claims arising from the State's sole negligence.
8. **EQUAL OPPORTUNITY CLAUSE:** The Contractor agrees to abide by the provisions of Title VI and VII of the Civil Rights Act of 1964 (42USC 2000e) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, religion, color, or national origin; and further agrees to abide by Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; 45 CFR 90 which prohibits discrimination on the basis of age; and Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities. Also, the Contractor agrees to abide by Utah's Executive Order, dated March 17, 1993, which prohibits sexual harassment in the work place.
9. **SEPARABILITY CLAUSE:** A declaration by any court, or any other binding legal source, that any provision of this contract is illegal and void shall not affect the legality and enforceability of any other provision of this contract, unless the provisions are mutually dependent.
10. **RENEGOTIATION OR MODIFICATIONS:** This contract may be amended, modified, or supplemented only by written amendment to the contract, executed by the same persons or by persons holding the same position as persons who signed the original agreement on behalf of the parties hereto, and attached to the original signed copy of the contract.
11. **DEBARMENT:** The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract), by any governmental department or agency. If the Contractor cannot certify this statement, attach a written explanation for review by the State. The Contractor must notify the State Director of Purchasing within 30 days if debarred by any governmental entity during the Contract period.
12. **TERMINATION:** Unless otherwise stated in the Special Terms and Conditions, this contract may be terminated, with cause by either party, in advance of the specified termination date, upon written notice being given by the other party. The party in violation will be given ten (10) working days after notification to correct and cease the violations, after which the contract may be terminated for cause. This contract may be terminated without cause, in advance of the specified expiration date, by either party, upon 90 days prior written notice being given the other party. On termination of this contract, all accounts and payments will be processed according to the financial arrangements set forth herein for approved services rendered to date of termination.
13. **NONAPPROPRIATION OF FUNDS:** The Contractor acknowledges that the State cannot contract for the payment of funds not yet appropriated by the Utah State Legislature. If funding to the State is reduced due to an order by the Legislature or the Governor, or is required by State law, or if federal funding (when applicable) is not provided, the State may terminate this contract or proportionately reduce the services and purchase obligations and the amount due from the State upon 30 days written notice. In the case that funds are not appropriated or are reduced, the State will reimburse Contractor for products delivered or services performed through the date of cancellation or reduction, and the State will not be liable for any future commitments, penalties, or liquidated damages.

- 14. SALES TAX EXEMPTION:** The State of Utah's sales and use tax exemption number is E33399. The tangible personal property or services being purchased are being paid from State funds and used in the exercise of that entity's essential functions. If the items being purchased are construction materials, they will be converted into real property by employees of this government entity, unless otherwise stated in the contract.
- 15. WARRANTY:** The contractor agrees to warrant and assume responsibility for all products (including hardware, firmware, and/or software products) that it licenses, contracts, or sells to the State of Utah under this contract for a period of one year, unless otherwise specified and mutually agreed upon elsewhere in this contract. The contractor (seller) acknowledges that all warranties granted to the buyer by the Uniform Commercial Code of the State of Utah apply to this contract. Product liability disclaimers and/or warranty disclaimers from the seller are not applicable to this contract unless otherwise specified and mutually agreed upon elsewhere in this contract. In general, the contractor warrants that: (1) the product will do what the salesperson said it would do, (2) the product will live up to all specific claims that the manufacturer makes in their advertisements, (3) the product will be suitable for the ordinary purposes for which such product is used, (4) the product will be suitable for any special purposes that the State has relied on the contractor's skill or judgment to consider when it advised the State about the product, (5) the product has been properly designed and manufactured, and (6) the product is free of significant defects or unusual problems about which the State has not been warned. Remedies available to the State include the following: The contractor will repair or replace (at no charge to the State) the product whose nonconformance is discovered and made known to the contractor in writing. If the repaired and/or replaced product proves to be inadequate, or fails of its essential purpose, the contractor will refund the full amount of any payments that have been made. Nothing in this warranty will be construed to limit any rights or remedies the State of Utah may otherwise have under this contract.
- 16. PUBLIC INFORMATION:** Contractor agrees that the contract will be a public document, and may be available for distribution. Contractor gives the State express permission to make copies of the contract and/or of the response to the solicitation in accordance with the State of Utah Government Records Access and Management Act. The permission to make copies as noted will take precedence over any statements of confidentiality, proprietary information, copyright information, or similar notation.
- 17. DELIVERY:** Unless otherwise specified in this contract, all deliveries will be F.O.B. destination with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage will remain with Contractor until final inspection and acceptance when responsibility will pass to the State except as to latent defects, fraud and Contractor's warranty obligations.
- 18. ORDERING AND INVOICING:** All orders will be shipped promptly in accordance with the delivery schedule. The Contractor will promptly submit invoices (within 30 days of shipment or delivery of services) to the State. The State contract number and/or the agency purchase order number shall be listed on all invoices, freight tickets, and correspondence relating to the contract order. The prices paid by the State will be those prices listed in the contract. The State has the right to adjust or return any invoice reflecting incorrect pricing.
- 19. PAYMENT:** Payments are normally made within 30 days following the date the order is delivered or the date a correct invoice is received, whichever is later. All payments to the Contractor will be remitted by mail unless paid by the State of Utah's Purchasing Card (major credit card).
- 20. PATENTS, COPYRIGHTS, ETC.:** The Contractor will release, indemnify and hold the State, its officers, agents and employees harmless from liability of any kind or nature, including the Contractor's use of any copyrighted or un-copyrighted composition, secret process, patented or un-patented invention, article or appliance furnished or used in the performance of this contract.
- 21. ASSIGNMENT/SUBCONTRACT:** Contractor will not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this contract, in whole or in part, without the prior written approval of the State.
- 22. DEFAULT AND REMEDIES:** Any of the following events will constitute cause for the State to declare Contractor in default of the contract:
1. Nonperformance of contractual requirements; 2. A material breach of any term or condition of this contract. The State will issue a written notice of default providing a ten (10) day period in which Contractor will have an opportunity to cure. Time allowed for cure will not diminish or eliminate Contractor's liability for damages. If the default remains, after Contractor has been provided the opportunity to cure, the State may do one or more of the following: 1. Exercise any remedy provided by law; 2. Terminate this contract and any related contracts or portions thereof; 3. Impose liquidated damages, if liquidated damages are listed in the contract; 4. Suspend Contractor from receiving future solicitations.
- 23. FORCE MAJEURE:** Neither party to this contract will be held responsible for delay or default caused by fire, riot, acts of God and/or war which is beyond that party's reasonable control. The State may terminate this contract after determining such delay or default will reasonably prevent successful performance of the contract.
- 24. PROCUREMENT ETHICS:** The Contractor understands that a person who is interested in any way in the sale of any supplies, services, construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, gratuity, contribution, loan or reward, or any promise thereof to any person acting as a procurement officer on behalf of the State, or who in any official capacity participates in the procurement of such supplies, services, construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization (63-56-1002, Utah Code Annotated, 1953, as amended).
- 25. CONFLICT OF TERMS:** Contractor Terms and Conditions that apply must be in writing and attached to the contract. No other Terms and Conditions will apply to this contract including terms listed or referenced on a Contractor's website, terms listed in a Contractor quotation/sales order, etc. In the event of any conflict in the contract terms and conditions, the order of precedence shall be: 1. State Standard Terms and Conditions; 2. State Additional Terms and Conditions; 3. Contractor Terms and Conditions.

UTAH DEPARTMENT OF TRANSPORTATION

AERONAUTICAL OPERATIONS DIVISION

**PROJECT APPLICATION AND GRANT AGREEMENT
FOR STATE AID FOR DEVELOPMENT OF PUBLIC AIRPORTS**

Part I - Project Information

MORGAN COUNTY (hereinafter called the “Sponsor”) hereby makes application to the Utah Department of Transportation (hereinafter called the “State”) for a grant of state funds pursuant to Title 72, Chapter 10, Aeronautics Act, for the purpose of aiding in financing an improvement project (hereinafter called the “project”) for the development of the **Morgan County**, (hereinafter called the “Airport”) located in **MORGAN_UT**.

It is proposed that the Project consists of the following described airport improvements or development:

Pavement Preservation

as shown on the attached map accompanied by a detailed engineering cost estimate showing each item in the Project by description, quantity, unit cost, total cost, engineering and contingencies. [The map will show (1) the boundaries of the Airport and all proposed additions thereto, together with the boundaries of all offsite areas owned or controlled by the Sponsor for airport purposes, and proposed additions thereto; (2) the location and nature of all existing and proposed airport facilities and structures (such as runways, taxiways, aprons, terminal buildings, hangars, and roads), including all proposed extensions and reductions of existing airport facilities; (3) the location of all existing and proposed non-aviation areas and of all existing and proposed improvements thereon including the access road; and (4) airport vicinity zoning.] It is understood that the State will approve in writing the project plans and specifications before start of construction.

The estimated total project is **\$115,294.44**. The requested State share is **\$103,765.00 (90.00%)**.

Other governmental agencies granting money to the project are **N/A**.

The Project engineer is intended to be **Wasatch Civil**

The FAA Project No. is **AIP-NA** (if applicable)

Part II - Representations

The Sponsor hereby represents and certifies as follows:

1. Legal Authority - The Sponsor has the legal power and authority to :
 - (1) do all things necessary in order to undertake and carry out the Project in conformity with applicable statutes;
 - (2) accept, receive, and disburse grants of funds from the State in aid of the Project;
 - (3) carry out all of the provisions of Parts III and IV of this document.
2. Funds - The Sponsor now has **\$11,529.44** available for use in defraying its share of the Project. The present status of these funds is as follows:

Part III – Sponsor’s Assurances

In consideration for grant monies made available to the airport, the Sponsor hereby covenants and agrees with the State, as follows:

1. The Sponsor will operate the Airport as such for the use and benefit of the public throughout the useful life of the facilities developed under this Project, but in any event for at least ten (10) years from the date hereof. In furtherance of this covenant, (but without limiting its general applicability and effect) the Sponsor specifically agrees that it will keep the airport open to all types, kinds, and classes of aeronautical use on fair and reasonable terms without discrimination between such types, kinds, and classes; provided, that the Sponsor may establish such fair, equal, and not unjustly discriminatory conditions to be met by all users of the Airport; and provided further, that the Sponsor may prohibit or limit any given type, kind or class of aeronautical use of the Airport if such action is necessary - (a) For safe and efficient use of the Airport; (b) To keep operation activities within acceptable noise levels; To serve the civil aviation needs of the public.

2. The Sponsor covenants and agrees that, unless authorized by the State, it will not either directly or indirectly, grant or permit any person, firm, or corporation the exclusive right at the Airport or at any other Airport now or hereafter owned or controlled by it, to conduct any aeronautical activities, including, but not limited to, charter flights, pilot training, aircraft rental and sightseeing, aerial photography, crop dusting, aerial advertising and surveying, air carrier operations, aircraft sales and services, sale of aviation petroleum products whether or not conducted in conjunction with other aeronautical activity, repair and maintenance of aircraft, sale of aircraft parts, and any other activities which because of their direct relationship to the operation of aircraft can be regarded as an aeronautical activity.

3. The Sponsor agrees that it will operate the Airport for the use and benefit of the public, on fair and reasonable terms, and without unjust discrimination. In furtherance of this covenant (but without limiting its general applicability and effect), the Sponsor specifically covenants and agrees:

a. That in its operation and the operation of all facilities on the airport, neither it nor any person or organization occupying space of facilities thereon will discriminate against any person or class of persons by reason of race, color, creed, or national origin in the use of any of the facilities provided for the public on the Airport.

b. That in any agreement, contract, lease, or other arrangement under which a right or privilege at the Airport is granted to any person, firm, or corporation to render to the public any service (including the furnishing or sale of any aeronautical parts, materials, or supplies) essential to the operation of aircraft at the Airport, the Sponsor will insert and enforce provisions requiring the contractor:

(1) To furnish said service on a fair, equal, and not unjustly discriminatory basis to all users thereof, and

(2) To charge fair, reasonable, and not unjustly discriminatory prices for each unit or service; Provided, that the contractor may be allowed to make reasonable and nondiscriminatory discounts, rebates, or other similar types of price reductions to volume purchasers.

c. That it will not exercise or grant any right or privilege which would operate to prevent any person, firm, or corporation operating aircraft on the Airport from performing any services on its own aircraft with its own employees (including, but not limited to maintenance and repair) that it may choose to perform.

d. In the event the Sponsor itself exercises any of the rights and privileges referred to in subsection b, the services involved will be provided on the same conditions as would apply to the furnishing of such services by contractors or concessionaires of the Sponsor under the provisions of such subsection b.

4. Nothing contained herein shall be construed to prohibit the granting or exercise of an exclusive right for the furnishing of non-aviation products and supplies or any service of a non-aeronautical nature or to obligate the Sponsor to furnish any particular non-aeronautical service at the Airport.

5. The Sponsor will operate and maintain in a safe and serviceable condition the Airport and all facilities thereon and connected therewith which are necessary to serve the aeronautical users of the Airport other than facilities owned or controlled by the United States, or the State, and will not permit any activity or uses thereon which would interfere with its use for airport purposes; Provided that nothing contained herein shall be construed to require that the Airport be operated for aeronautical uses during temporary periods when snow, flood, or other climatic conditions interfere with such operation and maintenance; and provided further, that nothing herein shall be construed as requiring the maintenance, repair, restoration or replacement of any structure or facility which is substantially damaged or destroyed due to an act of God or other condition or circumstance beyond the control of the Sponsor.

6. Insofar as it is within its power and reasonably possible, the Sponsor will, either by the acquisition and retention of easements or other interests in or rights for the use of land or airspace or by the adoption and enforcement of zoning regulations, prevent the construction, erection, alteration, or

growth of any structure, tree, or other object in the approach areas of the runways of the Airport, which would constitute an obstruction to air navigation according to the criteria or standards prescribed in Part 77 of the Federal Aviation Regulations. In addition, the Sponsor will not erect or permit the erection of any permanent structure or facility which would interfere materially with the use, operation, or future development of the Airport, in any portion of a runway approach area in which the Sponsor has acquired, or may hereafter acquire, property interests permitting it to so control the use made of the surface of the land. In addition the Sponsor will clear said area or areas of any existing structure or any natural growth that constitutes an obstruction to airspace within the standards established by said Part 77 unless exceptions to or deviations from the aforementioned obligations have been granted to it in writing by the State.

7. The Sponsor will furnish the State with such annual or special airport financial and operational reports as may be reasonably requested. Such reports may be submitted on forms furnished by the State, or may be submitted in such manner as the Sponsor elects as long as the essential data is furnished. The Airport and all Airport records and documents affecting the Airport, including deeds, leases, operation and use agreements, regulations, and other instruments will be made available for inspection and audit by the State, or his duly authorized representative upon reasonable request. The sponsor will furnish to the State a true copy of any such documents.

8. The Sponsor will furnish Utah's Division of Aeronautics on a semi-annual basis a list of all aircraft which have been based at the airport for more than 6 months, out of the last 12 months. The list shall include the aircraft tail numbers with the owner's current name and address.

9. The Sponsor will not enter into any transaction which would operate to deprive it of any of the rights and powers necessary to perform any or all of the covenants made herein, unless by such transaction the obligation to perform all such covenants is assumed by another public agency found by the State to be eligible to assume such obligations and having the power, authority, and financial resources to carry out all such obligations. If an arrangement is made for management or operation of the Airport by any agency or person other than the Sponsor or an employee of the Sponsor, the Sponsor will reserve sufficient rights and authority to ensure that the Airport will be operated and maintained in accordance with these covenants.

10. The Sponsor will keep up to date, by amendment, the attached map of the Airport showing:

- (1) The boundaries of the Airport and all proposed additions thereto, together with the boundaries of all offsite areas owned or controlled by the Sponsor for airport purposes, and proposed additions thereto;
- (2) The location and nature of all existing and proposed airport facilities and structures (such as runways, taxiways, aprons, terminal buildings, hangars, and roads), including all proposed extensions and reductions of existing airport facilities; and
- (3) The location of all existing and proposed non-aviation areas and of all existing improvements thereon, including the access road, said attached map, and each amendment,

revision, or modification thereof, shall be subject to the approval of the State which approval shall be evidenced by the signature of a duly authorized representative of the State on the face thereof. The Sponsor will not make or permit the making of any changes or alterations in the Airport or any of its facilities that might adversely affect the safety, utility, or efficiency of the Airport.

(4) Airport vicinity zoning.

11. Insofar as is within its power and to the extent reasonable, the Sponsor will take action to restrict the use of land adjacent to or in the immediate vicinity of the Airport to activities and purposes compatible with normal airport operations including landing and takeoff of aircraft.

12. The Sponsor will not dispose of, or abandon in any manner, any portion of the Airport shown on the approved map without the written consent of the State.

13. It is understood and agreed that as to the land acquired or to be acquired for future development of the airport, the Sponsor will construct and complete thereon a useful and usable facility consistent with the State Airport System Plan not later than the time of forecasted need; and if the land so acquired or any part thereof, is not used within the forecast period for the purpose for which it was acquired, the Sponsor will refund the State share of acquisition cost or fair market value of the land, whichever is greater, plus the State share of net revenue, at the time of sale or expiration of the period stated in this agreement. It is further understood and agreed that the Sponsor will deposit all net revenues derived from the interim use of the land into a special fund to be used exclusively for approved items of airport development, but in no case may the State share of such funds be used to match State aid funds in future grants. It is still further understood and agreed that the Sponsor will not dispose of the land by sale, lease, or otherwise without the prior consent and approval of the State.

14. The Sponsor will maintain, at its own expense, the following aeronautical use items and activities:

- (1) A standard, mounted windsock for observation of wind direction and velocity from the ground and while airborne together with a standard segmented circle, both in good repair.
- (2) Enforcement of zoning in the vicinity of airports to minimize environmental problems associated with aeronautical uses.
- (3) A current license issued by the State designating the Airport for public use.
- (4) Runway or boundary lights in good repair and on from dusk to dawn of each calendar day.
- (5) The runway, taxiways, and apron in a state of good repair which would include annual crack filling and mowing of vegetation at least 15 feet outside of hard surfaced areas as necessary to maintain a weed height of not more than 12 inches.

(6) The boundary fence, when in place, in a state of good repair.

(7) The main runway, associated taxiway and apron to be cleared of snow as soon as practical after a snowstorm and the airport to remain open for use during these months.

15. It is understood that the State will participate in the amount of grant monies herein mentioned in the engineering estimate or in the herein mentioned per cent share of the actual project cost, whichever is least.

16. In the event the State does not grant monies under this application, the covenants herein mentioned shall not become effective.

17. Sponsor shall have no authorization to bind the State of Utah or the Utah Department of Transportation, or its Aeronautical Operations Division to any agreement, settlement, liability or understanding whatsoever, nor to perform any acts as agent for the State of Utah, except as herein expressly set forth.

18. Sponsor hereby agrees to indemnify and save harmless the State of Utah, Utah Department of Transportation, and Aeronautical Operations Division, and their officers, agents, and employees from and against any and all loss, damages, injury, and liability, and any claims therefore, including claims for personal injury or death, damages to personal property and liens of workmen and materialmen, howsoever caused, resulting directly or indirectly from the performance of this agreement or from the use or operation of the airport improvements and facilities being purchased, constructed or otherwise developed under this agreement.

Part IV - Project Agreement and Acceptance

If the Project or any portion thereof is approved by the State, and State aid for such approved Project is accepted by the Sponsor, it is understood and agreed that all airport development included in such Project will be accomplished in accordance with the plans and specifications for such development, as approved by the State, and the herein assurances with respect to the Project and the Airport.

IN WITNESS WHEREOF, The parties hereto do hereby ratify and adopt all statements, representatives, warranties, covenants, and agreements contained or referenced herein and do hereby cause this document to be executed in accordance with the terms and conditions here of.

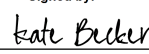
Executed for the Sponsor on: 7/27/2026

(SEAL)

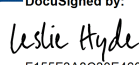


MORGAN COUNTY

(Name of Sponsor)

By 
Signed by:
F907222416C044F...

Title **Morgan County Administrative Manager**
Kate Becker

Attest 
DocuSigned by:
F155F3A8C99E460...

Leslie Hyde, Leslie A. Hyde
Clerk/Auditor/Recorder

CERTIFICATE OF SPONSOR'S ATTORNEY

I, **Garrett Smith**, acting as Attorney for **MORGAN COUNTY** (herein referred to as the "Sponsor") do hereby certify:

That I have examined the foregoing document and the proceedings taken by said Sponsor relating thereto, and find that the Acceptance thereof by said Sponsor has been duly authorized and that the execution thereof is in all respects due and proper and in accordance with the laws of the State of Utah, and further that, in my opinion, said Agreement constitutes a legal and bind obligation of the Sponsor in accordance with the terms thereof.

Dated at _____.

Title **County Attorney**

AERONAUTICAL OPERATIONS DIVISION

Director

APPROVED:

Finance

NOTICE OF AWARD

DATED: June 10, 2026

TO: Morgan Pavement

ADDRESS: 625 S. Main Street Clearfield, UT 84015

PROJECT: Airport Pavement Maintenance Project

You are notified that your Bid dated 5/28/2026, for the above Contract has been considered. You are the apparent Successful Bidder and have been awarded a Contract for the **Airport Pavement Maintenance Project**. The Contract Price of your Contract is Nintey-One Thousand, Twenty-Five and 00/100's Dollars (\$91,025.00).

Actual total price will be based on the sum of work items completed (as measured in the field) multiplied by the unit prices for each item.

One copy of each of the proposed Contract Documents (except Drawings) accompanies this Notice of Award. Three sets of the Drawings will be delivered separately or otherwise made available to you immediately.

You must comply with the following conditions precedent within 10 days of the date of this Notice of Award:

1. Submit a Signed Contract Agreement
2. Submit a Payment Bond
3. Submit a Performance Bond
4. Submit Certificates of Insurance as specified in General and Supplementary Conditions

Failure to comply with these conditions within the time specified will entitle OWNER to consider your Bid in default, to annul this Notice of Award and to declare your Bid security forfeited.

Morgan County Airport
(OWNER)

(AUTHORIZED SIGNATURE)

(TITLE)

2026 Fall Growth Grant Recommendations from CEO

Business Name	Requested	Description	Final
Milk Barn Creamery LLC	985.47	Shake Machine	\$ 328.49
Higbee Honey	5,000.00	Website Upgrades & Design	\$ 5,000.00
Wasatch Caregivers dba Wasatch Senior Care	6,600.00	Digital and Print Marketing	\$ 4,400.00
Hooked Up Plumbing	5,000.00	Digital Advertising and Trade Specific Tools	\$ 4,000.00
Achieve Fitness of Morgan	10,000.00	Building Expansion	\$ 7,750.00
Climbaxe Tree Services	5,000.00	Website and click optimization	\$ 5,000.00
Debs spicy pie	50,000.00	Website Creation	\$ 5,000.00
Phoenix house DbA The Mountain Green Bean	5,000.00	Digital Drive Thru Menu	\$ 2,280.00
Destination Sports, LLC	5,016.00	Intern	\$ 3,762.00
Brighten Blades	4,500.00	Facebook Advertising	\$ 3,285.00
Confluence Consulting LLC	5,000.00	CRM, Advertising, and Equipment	\$ 2,760.00
Haro Construction of Utah	10,800.00	Trade Specific Tools	\$ 3,350.00
Corner Cove Wellness	5,000.00	Body Scanner	\$ 3,250.00
			\$50,165.49

Kate Becker

From: Korey Adams <koreyadams@adamsconstructionservicesut.com>
Sent: Friday, August 7, 2026 9:39 AM
To: Kate Becker
Subject: Re: Safe Room & Closet-Clerks Addition

CAUTION: This email originated from outside of Morgan County. Do not click links or open attachments unless you recognize the sender and know the content is safe. If you are unsure please contact Jeremy or Brandon.

Kate,

Following our assessment after removing the existing shelving in the safe room, I am reaching out to update you on the scope of work for the requested wall demolition and framing modifications.

Our team has mapped out the required work as follows:

- **Wall Demolition:** Demolition and disposal of the 10-inch thick concrete and brick wall (estimated 3-day duration due to material density). Remove the file shelving and stack it in the auditorium. Removing the shelving has been completed.
- **Ceiling Tile Adjustments:** Potential repair or replacement of ceiling tiles directly impacted by the wall removal.
- **Framing:** Removal of one existing door and framing out two new door openings. (Morgan County Employees will remove the safe door). Please have them remove it on Tuesday August 11.
- **Sheetrock Repair:** Install sheetrock in newly framed door areas and repair plaster walls as necessary.
- **Flooring:** Carpet Tiles and rubber base will need to be installed.
- **Painting:** The room will need to be painted before carpet is installed.
- **Electrical:** This scope excludes all electrical tasks. We assume no electrical lines need to be moved to demo the wall, no adjustments to lighting, outlets, or switches. Excludes Data line removal or installation.
- **HVAC:** This scope does not include adding or adjusting any HVAC units.

Based on our evaluation, the complexity of removing the concrete/brick wall—along with the required ceiling repairs, framing, flooring, sheetrock, Paint and carpet tiles—will exceed the currently available \$12,000 contingency fund.

To keep the project moving forward, we require a formal Notice to Proceed acknowledging that the total cost will exceed the current \$12,000 allocation.

Please let me know if you would like to schedule a quick call or walk the space together before issuing the authorization.

Regards,

Owner Authorizing Signature: _____



2026 BUDGET CHANGE FORM

Date	08/11/2026
Department	Fleet: Ambulance
Department Head Signature	Kate Becker
Amount	346,000
Move from GL Account#	10-2951-000-000 General Fund Balance
Move to GL Account #	10-4460-250-550 Ambulance Vehicles

Brief Description

Morgan County Commission approved the purchase of a new ambulance during budget meetings in October of 2025. The anticipated delivery date was 18 months from purchase agreement however it is going to be delivered in 2026.

Clerk/Auditor Use Only

Date Entered:
Date Commission Approved:

Oct 2027

Approved to order
\$346,000
will
pay for
in 2027

PSS / PROFESSIONAL SALES AND SERVICE, L.C.

Quality Emergency Vehicles Since 1974

August 11, 2025

Morgan County
41 North State Street
Morgan UT, 84050

To Whom It May Concern:

Professional Sales and Service, LC respectfully provides the Morgan County the following proposal for a new ambulance vehicle. We appreciate the opportunity to work with you now and look forward to helping you with your ambulance needs in the future.

The following proposal reflects New Type I ambulances the proposal is as follows:

One 2026 Horton 603 Type I 4x4 Custom Ambulances Mounted on 2026 Ford F-550 4x4 Diesel Chassis

The module body will be 167" long and have an interior height of 72" inches. It will be mounted on a 2026 Ford F-550 4X4 with a Diesel Motor dual rear wheel cab/chassis. This proposal includes Horton's electrical system: The most advanced electrical system available which incorporates solid-state electronics with Multiplexing technology. It also includes weight saving all-aluminum module body, NO-wood construction, aluminum cabinetry, electrical system diagnostic testing, digital computer consoles, privacy windows, LED lighting package and much more. Full specification attached.

Take a look at Horton Emergency Vehicles (HEV) and you will see why they are so well regarded in the ambulance industry and among the finest available anywhere. A Horton emergency vehicle is BUILT TO WITHSTAND the rigors of ambulance service. Horton ambulances are tested and engineered to be incredibly structurally sound which provides the EMS crew and patient with a SAFER WORKING ENVIRONMENT. They are currently the only manufacturer with an ongoing crash simulation testing program to test things like cabinet mounting stability, door structure & latching strength, and body mounting solidity. ALUMINUM CABINETS SAVE PAYLOAD and are much more DURABLE than wood. An ambulance built to a higher quality standard will provide REDUCED OPERATING COSTS over the many years the vehicle is in service!! When it comes to quality, durability, customization, and safety, Horton continues to be a leader in the ambulance manufacturing industry.

PSS SHOWROOM

1720 Indiana Ave, Salt Lake City, UT 84104
(801) 977-3961 Phone <> (801) 977-3969 Fax

PSS / PROFESSIONAL SALES AND SERVICE, L.C.

Quality Emergency Vehicles Since 1974

PRICING PAGE

<u>Ambulance Price.....</u>	<u>\$310,149.00</u>
<u>Shipping.....</u>	<u>\$4,800.00</u>
<u>Styker Power Load System.....</u>	<u>\$30,795.00</u>
<u>Total Delivered Price Each Ambulance.....</u>	<u>\$345,744.00</u>

PROPOSAL CONDITIONS

F.O.B. POINT: Morgan UT, 84050

DELIVERY: Do to current and ongoing national supply chain issues specifically in regard to chassis availability. We will be providing estimated delivery times only. Currently Horton standard lead time is approximately 18 months (pending chassis). Please note all delivery times are quoted barring any delays due to strikes, availability of component parts (including chassis), or acts of God

SERVICE: Professional Sales & Service has been selling and servicing ambulances since 1975. We have factory trained technicians and a large inventory of parts, so you know that in the unlikely event of a problem we are only a phone call away.

PAYMENT TERMS: Payment due upon delivery and acceptance of vehicle by the Morgan County

PSS SHOWROOM

1720 Indiana Ave, Salt Lake City, UT 84104
(801) 977-3961 Phone <> (801) 977-3969 Fax

PSS / PROFESSIONAL SALES AND SERVICE, L.C.

Quality Emergency Vehicles Since 1974

** Pre-Payment discounts available upon request.

WARRANTY:

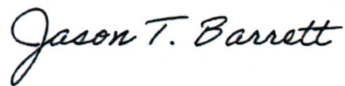
Horton Emergency Vehicles feature one of the most progressive, no-nonsense warranties around. Horton does not pro rate their warranties so there are no surprises should you ever need it.

Unless accepted within Sixty (60) days from the above date, the right to withdraw this proposal is reserved. If there are any additions/deletions to our bid, please contact me for pricing details or credits.

We are confident you will be completely satisfied with the quality Horton ambulance and the service which PSS provides.

Respectfully Submitted,

Professional Sales and Service, LC



Jason Barrett - Utah Sales

Morgan County agrees to purchase the vehicle detailed in this proposal, from Professional Sales and Service, L.C. and understands and agrees with the terms specified within these documents.

_____	_____	_____
Authorized by (Print name)	Signed	Date

Please let us know if you have any questions regarding this proposal. We are happy to assist you in any way that we can.

PSS SHOWROOM

1720 Indiana Ave, Salt Lake City, UT 84104
(801) 977-3961 Phone <> (801) 977-3969 Fax

Kelli Petty

Account # 433157827

Order Details

[Back to EDDM® Tool](#)

Order Number
10640125

Created
06/03/2026

Nickname
Morgala Days Rodeo 2026 - SWebr, Uinta, Vally
[Edit](#)

Delivery Information
4877 Mailpieces
3 Post Office™ Drop-Offs
Payment Method
Paid Online

ZIP Code(s)™
84317, 84405, 84403

Drop-Off Date
06/03/2026

Routes	Mailpieces	Post Office™ Drop-Off Location(s)	Cost	Status
2	1051	HUNTSVILLE 7785 E 500 S HUNTSVILLE, UT 84317	\$259.60	
4	2726	OGDEN 3680 PACIFIC AVE OGDEN, UT 84401	\$673.32	
2	1100	MOUNT OGDEN 1145 E 4600 S OGDEN, UT 84403	\$271.70	
Total			\$1204.62	

[Repeat Order](#)

[Add to Favorites](#)

[Reprint Forms](#)

Feedback

What do I do next?

1. Double-check your mailpieces.

We have specific requirements for mailpiece size and format.

- Use our [Mailpiece Size Checker](#) or read our [EDDM Quick Reference](#) guide to make sure your mailings meet size requirements.
- Include the approved EDDM Retail® Indicia (the postage payment mark that takes the place of a regular postage stamp or meter stamp). Get more information on [EDDM Postage](#).
- Need help? Our third-party vendors can help you format, design, print, and prepare your mailing to meet Postal Service™ standards. [Find a Local Printer](#).

2. Prepare your mailing bundle(s).

**MORGAL DAYS
RODEO**

★ SINCE 1949 ★
MORGAN, UTAH

GAMES, FOOD & FUN FOR THE WHOLE FAMILY

**FOR DETAILS VISIT
MORGALDAYSRODEO.ORG**

*** Ben James - Bull Fighter/ Clown Act ***



scan for tickets

*** Food Trucks * Vendors * Mechanical Bull ***

WESTERN SWING DANCING

SATURDAY NIGHT AFTER THE RODEO

(INCLUDED WITH RODEO TICKET PURCHASE)

PROUDLY HOSTED BY

MORGAN



**RODEO CLUB
UHSRA**



RODEO COMPANY



Explore Morgan



MorganValley

Make us your go to spot!

801.829.8808

Box 100 Morgan Valley, UT 84050

PRINTED BY MORGAN VALLEY PRINTS



MORGALA

DAYS

ROCKY MTN.

PRO-RODEO

**ON-LINE
TICKETS**

\$10

**GENERAL ADMISSION
\$12 RESERVED SEATING**

POSTAL CUSTOMER

PSRT STD
ECRWSS
U.S. POSTAGE
PAID
EDDM Retail

FRIDAY

&

SATURDAY

JUNE

12 & 13

7PM

MUTTON BUSTIN'

PRE-SHOW

6:30PM

**Morgan County Fairgrounds
Morgan, Utah**



**UTAH DEPARTMENT OF AGRICULTURE AND FOOD
STATE OF UTAH GRANT AGREEMENT**

Contract # _____

Vendor # 83870FB

This Agreement is between the Utah Department of Agriculture and Food (UDAF) and the following entity Grantee:

**Morgan County
48 W Young Street
Morgan, Utah 84050**

1. **GENERAL PURPOSE OF AGREEMENT:** Provide Predation Management as outlined in Attachment A, Morgan County Predation Management Plan.
2. **AGREEMENT PERIOD:** Effective Date: **7/1/26**; Termination Date: **6/30/27**; unless terminated early or extended in accordance with the terms and conditions of this Agreement.
3. **AGREEMENT COSTS:** The total Agreement amount due is **\$21,100**. This Agreement authorizes UDAF to reimburse 50% of the total costs up to \$10,050.
4. **AGREEMENT DUE DATE:** This Agreement, signed by Grantee, and all PDCF funds must be received at the UDAF main office no later than **October 31, 2026**.
5. The following attached documents are hereby incorporated by reference into this Agreement:
ATTACHMENT A: County Predation Management Plan
ATTACHMENT B: UDAF Program Participation Letter
ATTACHMENT C: Producer County Match Form
ATTACHMENT D: Standard Terms and Conditions for Goods and/or Services (both parties' government entities)
6. Any conflicts between Attachment D and other Attachments shall be resolved in favor of Attachment D.
7. **ADDITIONAL PROVISIONS:**
 - a. This Agreement is subject to the laws of the State of Utah, and to all other federal, state and local laws, regulations, or actions applicable to the services authorized by this Agreement.
 - b. Each signatory below represents that he or she has the requisite authority to enter into this Agreement.
 - c. This Agreement is not fully executed until all approving authorities listed below have signed this Agreement.

By signing below, the parties hereby execute this Agreement:

GRANTEE

Grantee's Signature

Date

Grantee's Name and Title

UDAF/STATE

Grantor's Signature

Date

UDAF Admin Services

Date

Division of Finance

Date

Morgan County Predation Management Plan -2027

Thank you for the contract allowing the Department of Agriculture and Food to match up to 50% of the County's contracted amount for predation management in Morgan County.

The work plan is as follows:

Morgan County will participate in the Predator Damage Control Fund (PDCF) program at the rate of \$21,100 annually. UDAF will reimburse the county for 50% of the request, not to exceed the total annual contract portion of \$10,050. The funds provided by the County and producers will be deposited into the PDCF account, by the Utah Wool Growers Association (UWGA). These funds will be allocated and used within Morgan County and will be administered by UDAF for aerial predator management.

Please make checks payable to:
PDCF
and mail to:
Utah Department of Agriculture and Food
P.O. Box 146500 Salt Lake City, Utah 84114-6500

Included with this paperwork is a Predator County Match Form to log County and producer's contributions to this program. Please return this form with payment to better provide accountability to the program participants.



State of Utah

SPENCER J. COX
GovernorDEIDRE M. HENDERSON
Lieutenant Governor

Department of Agriculture and Food

KELLY PEHRSON
CommissionerTROY FORREST
Deputy CommissionerPHIL CROWTHER
Deputy Director, Predator ControlCOLE SELMAN
Predator Control Program Manager

To: Predator Damage Control Fund (PDCF) participants

Subject: October 31, 2026 Deadline to receive matching funds for predator damage management

Each year the Utah Department of Agriculture and Food (UDAF) and the Division of Wildlife Resources (DWR) fund a program in which producers can contribute funds toward a predator damage management program, PDCF, and have their funds matched through the Counties. The program is administered by UDAF in cooperation with DWR. To maximize the allotted funds and to provide the best possible service we can, we are asking that all PDCF funds from the Counties be sent in and received at the UDAF main office no later than October 31, 2026. If we do not receive your funds and signed contract by this date, your potential matching funds will become available to other counties for use, and your county may NOT be able to participate in the matching fund program.

**Please make checks payable to
PDCF
and mail to
Utah Department of Agriculture and Food
P.O. Box 146500
Salt Lake City, Utah 84114-6500**

Each year there are funds "left on the table" that could be used to benefit livestock producers within the Counties. This is due to Counties signing the contracts for a specific amount of money, and then not fully funding or not providing the funds for them at all. Any unpaid contract funds will be available for other counties to use after the deadline of January 1, 2027; these funds will be available until exhausted. Any funds distributed after the deadline will be allocated as decided by the Wool Grower's Presidency.

Also, you will be receiving a tracking form with the contract. This form will help us track which producer's put money towards the program and thus, we can make sure that we provide the amount of service they paid for. This form is required to be with the payment when submitted.

Thank you in advance for your cooperation, I think this will enable us to provide more services to you and will maximize the funds set aside for predator management.

If you have any questions, please feel free to contact me at the number listed below.

Cole Selman
Predator Control Program Manager
(385) 222-6790

ATTACHMENT D: STATE OF UTAH AGENCY STANDARD TERMS AND CONDITIONS FOR GOODS AND/OR SERVICES

These terms and conditions may only be used when both parties are government entities or political subdivisions as defined in the Utah Government Immunity Act.

1. **DEFINITIONS:** The following terms shall have the meanings set forth below:
 - a) **"Confidential Information"** means information that is deemed as confidential under applicable state and federal laws, and personal data as defined in Utah Code 63A-19-101. The State Entity reserves the right to identify, during and after this Contract, additional reasonable types of categories of information that must be kept confidential under federal and state laws.
 - b) **"Contract"** means the Contract Signature Page(s), including all referenced attachments and documents incorporated by reference. The term "Contract" shall include any purchase orders that result from this Contract.
 - c) **"Contract Signature Page(s)"** means the State of Utah cover page(s) that the State Entity and Contractor signed.
 - d) **"Contractor"** means the individual or entity delivering the Procurement Item identified in this Contract. The term "Contractor" shall include Contractor's agents, officers, employees, and partners.
 - e) **"Custom Deliverable"** means the Work Product that Contractor is required to deliver to the State Entity under this Contract.
 - f) **"Goods"** means all types of tangible personal property, including but not limited to materials, supplies, Custom Deliverable, and equipment that Contractor is required to deliver to the State Entity under this Contract.
 - g) **"Procurement Item"** means Goods, a supply, Services, Custom Deliverable, construction, or technology that Contractor is required to deliver to the State Entity under this Contract.
 - h) **"Response"** means the Contractor's bid, proposals, quote, or any other document used by the Contractor to respond to the State Entity's Solicitation.
 - i) **"Services"** means the furnishing of labor, time, or effort by Contractor pursuant to this Contract. Services include those professional services identified in Section 63G-6a-103 of the Utah Procurement Code
 - j) **"Solicitation"** means an invitation for bids, request for proposals, notice of a sole source procurement, request for statement of qualifications, request for information, or any document used to obtain bids, proposals, pricing, qualifications, or information for the purpose of entering into this Contract.
 - k) **"State Entity"** means the department, division, office, bureau, agency, or other organization identified on the Contract Signature Page(s).
 - l) **"State of Utah"** means the State of Utah, in its entirety, including its institutions, agencies, departments, divisions, authorities, instrumentalities, boards, commissions, elected or appointed officers, employees, agents, and authorized volunteers.
 - m) **"Subcontractors"** means a person under contract with a contractor or another subcontractor to provide services or labor for design or construction, including a trade contractor or specialty contractor.
2. **GOVERNING LAW AND VENUE:** This Contract shall be governed by the laws, rules, and regulations of the State of Utah. Any action or proceeding arising from this Contract shall be brought in a court of competent jurisdiction in the State of Utah. Venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County.
3. **LAWS AND REGULATIONS:** At all times during this Contract, Contractor and all Procurement Items delivered and/or performed under this Contract will comply with all applicable federal and state constitutions, laws, rules, codes, orders, and regulations, including applicable licensure and certification requirements. If this Contract is funded by federal funds, either in whole or in part, then any federal regulation related to the federal funding, including CFR Appendix II to Part 200, will supersede this Attachment A.
4. **RECORDS ADMINISTRATION:** Contractor shall maintain or supervise the maintenance of all records necessary to properly account for Contractor's performance and the payments made by the State Entity to Contractor under this Contract. These records shall be retained by Contractor for at least six (6) years after final payment, or until all audits initiated within the six (6) years have been completed, whichever is later. Contractor agrees to allow, at no additional cost, the State of Utah, federal auditors, State Entity staff, or their designees, access to all such records during normal business hours and to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Contract.
5. **PERMITS:** If necessary Contractor shall procure and pay for all permits, licenses, and approvals necessary for the execution of this Contract.
6. **CERTIFY REGISTRATION AND USE OF EMPLOYMENT "STATUS VERIFICATION SYSTEM":** INTENTIONALLY DELETED
7. **CONFLICT OF INTEREST:** INTENTIONALLY DELETED
8. **INDEPENDENT CONTRACTOR:** Contractor and Subcontractors, in the performance of this Contract, shall act in an independent capacity and not as officers or employees or agents of the State Entity or the State of Utah.
9. **CONTRACTOR RESPONSIBILITY:** Contractor is solely responsible for fulfilling the contract, with responsibility for all Procurement Items delivered and/or performed as stated in this Contract. Contractor shall be the sole point of contact regarding all contractual matters. Contractor must incorporate Contractor's responsibilities under this Contract into every subcontract with its Subcontractors that will provide the Procurement Item(s) to the State Entity under this Contract. Moreover, Contractor is responsible for its Subcontractors compliance under this Contract.
10. **INDEMNITY:** Both parties to this agreement are Utah governmental entities as defined in the Utah Governmental Immunity Act (Utah Code Ann. 63G-7-101 et. seq.). Nothing in this Contract shall be construed as a waiver by either or both parties of any rights, limits, protections or defenses provided by the Act. Nor shall this Contract be construed, with respect to third parties,

as a waiver of any governmental immunity to which a party to this Contract is otherwise entitled. Subject to and consistent with the Act, each party will be responsible for its own actions or negligence and will defend against any claims or lawsuit brought against it. There are no indemnity obligations between these parties.

11. **EMPLOYMENT PRACTICES:** Contractor agrees to abide by the following federal and state employment laws, including: (i) Title VI and VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e), which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services on the basis of race, religion, color, or national origin; (ii) Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; (iii) 45 CFR 90, which prohibits discrimination on the basis of age; (iv) Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990, which prohibits discrimination on the basis of disabilities; and (v) Utah's Executive Order 2019-1, dated February 5, 2019, which prohibits unlawful harassment in the workplace. Contractor further agrees to abide by any other laws, regulations, or orders that prohibit the discrimination of any kind by any of Contractor's employees.
12. **AMENDMENTS:** This Contract may only be amended by the mutual written agreement of the parties, provided that the amendment is within the Scope of Work of this Contract and is within the scope/purpose of the original solicitation for which this Contract was derived. The amendment will be attached and made part of this Contract. Automatic renewals will not apply to this Contract, even if listed elsewhere in this Contract.
13. **DEBARMENT:** Contractor certifies that it is not presently nor has ever been debarred, suspended, proposed for debarment, or declared ineligible by any governmental department or agency, whether international, national, state, or local. Contractor must notify the State Entity within thirty (30) days if debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in any contract by any governmental entity during this Contract.
14. **TERMINATION:** This Contract may be terminated, with cause by either party, in advance of the specified expiration date, upon written notice given by the other party. The party in violation will be given ten (10) days after written notification to correct and cease the violations, after which this Contract may be terminated for cause immediately and subject to the remedies below. This Contract may also be terminated without cause (for convenience), in advance of the specified expiration date, by the either party, upon thirty (30) days written termination notice being given to the other party. The State Entity and the Contractor may terminate this Contract, in whole or in part, at any time, by mutual agreement in writing.

On termination of this Contract, all accounts and payments will be processed according to the financial arrangements set forth herein for approved and conforming Procurement Items ordered prior to date of termination. In no event shall the State Entity be liable to the Contractor for compensation for any Good neither requested nor accepted by the State Entity. In no event shall the State Entity's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State Entity for any damages or claims arising under this Contract.
15. **NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW:** Upon thirty (30) days written notice delivered to the Contractor, this Contract may be terminated in whole or in part at the sole discretion of the State Entity, if the State Entity reasonably determines that: (i) a change in Federal or State legislation or applicable laws materially affects the ability of either party to perform under the terms of this Contract; or (ii) that a change in available funds affects the State Entity's ability to pay under this Contract. A change of available funds as used in this paragraph includes, but is not limited to a change in Federal or State funding, whether as a result of a legislative act or by order of the President or the Governor.

If a written notice is delivered under this section, the State Entity will reimburse Contractor for the Procurement Item(s) properly ordered and/or services properly performed until the effective date of said notice. The State Entity will not be liable for any performance, commitments, penalties, or liquidated damages that accrue after the effective date of said written notice.
16. **SALES TAX EXEMPTION:** The Procurement Item(s) under this Contract will be paid for from the State Entity's funds and used in the exercise of the State Entity's essential functions as a State of Utah entity. Upon request, the State Entity will provide Contractor with its sales tax exemption number. It is Contractor's responsibility to request the State Entity's sales tax exemption number. It is also Contractor's sole responsibility to ascertain whether any tax deduction or benefits apply to any aspect of this Contract.
17. **WARRANTY OF PROCUREMENT ITEM(S):** Contractor warrants, represents and conveys full ownership and clear title, free of all liens and encumbrances, to the Procurement Item(s) delivered to the State Entity under this Contract. Contractor warrants for a period of one (1) year that: (i) the Procurement Item(s) perform according to all specific claims that Contractor made in its Response; (ii) the Procurement Item(s) are suitable for the ordinary purposes for which such Procurement Item(s) are used; (iii) the Procurement Item(s) are suitable for any special purposes identified in the Contractor's Response; (iv) the Procurement Item(s) are designed and manufactured in a commercially reasonable manner; (v) the Procurement Item(s) are manufactured and in all other respects create no harm to persons or property; and (vi) the Procurement Item(s) are free of defects. Unless otherwise specified, all Procurement Item(s) provided shall be new and unused of the latest model or design.

Remedies available to the State Entity under this section are limited to the following: Contractor will repair or replace Procurement Item(s) at no charge to the State Entity within a reasonable time of any written notification informing Contractor of the Procurement Item(s) not performing as required under this Contract. If the repaired and/or replaced Procurement Item(s) prove to be inadequate, or fail its essential purpose, Contractor will refund the full amount of any payments that have been made.
18. **CONTRACTOR'S INSURANCE RESPONSIBILITY: INTENTIONALLY DELETED**
19. **RESERVED.**
20. **PUBLIC INFORMATION:** Contractor agrees that this Contract, related purchase orders, related pricing documents, and invoices will be public documents and may be available for public and private distribution in accordance with the State of Utah's Government Records Access and Management Act (GRAMA). Contractor gives the State Entity and the State of Utah express permission to make copies of this Contract, related sales orders, related pricing documents, and invoices in accordance with GRAMA. Except for sections identified in writing by Contractor and expressly approved by the State of Utah Division of Purchasing and General Services, Contractor also agrees that the Contractor's Response will be a public

document, and copies may be given to the public as permitted under GRAMA. The State Entity and the State of Utah are not obligated to inform Contractor of any GRAMA requests for disclosure of this Contract, related purchase orders, related pricing documents, or invoices.

21. **DELIVERY:** All deliveries under this Contract will be F.O.B. Destination Freight Prepaid and Allowed, unless specifically negotiated otherwise and explicitly written in this contract, with all transportation and handling charges paid for by Contractor. Responsibility and liability for loss or damage will remain with Contractor until final inspection and acceptance when responsibility will pass to the State Entity, except as to latent defects or fraud. Contractor shall strictly adhere to the delivery and completion schedules specified in this Contract.
22. **ACCEPTANCE AND REJECTION:** The State Entity shall have thirty (30) days after delivery of the Procurement Item(s) to perform an inspection of the Procurement Item(s) to determine whether the Procurement Item(s) conform to the standards specified in the Solicitation and this Contract prior to acceptance of the Procurement Item(s) by the State Entity.
- If Contractor delivers nonconforming Procurement Item(s), the State Entity may, at its option and at Contractor's expense: (i) return the Procurement Item(s) for a full refund; or (ii) require Contractor to promptly correct or replace the nonconforming Procurement Item(s). Contractor shall not redeliver corrected or rejected Procurement Item(s) without: first, disclosing the former rejection or requirement for correction; and second, obtaining written consent of the State Entity to redeliver the corrected Procurement Item(s). Repair, replacement, and other correction and redelivery shall be subject to the terms of this Contract.
23. **INVOICING:** Contractor will submit invoices within thirty (30) days of the delivery date of the Procurement Item(s) to the State Entity. The contract number shall be listed on all invoices, freight tickets, and correspondence relating to this Contract. The prices paid by the State Entity will be those prices listed in this Contract, unless Contractor offers a prompt payment discount within its Response or on its invoice. The State Entity has the right to adjust or return any invoice reflecting incorrect pricing.
24. **PAYMENT:** Payments are to be made within thirty (30) days after a correct invoice is received. All payments to Contractor will be remitted by mail, electronic funds transfer, or the State of Utah's Purchasing Card (major credit card). If payment has not been made after sixty (60) days from the date a correct invoice is received by the State Entity, then interest may be added by Contractor as prescribed in the Utah Prompt Payment Act. The acceptance by Contractor of final payment, without a written protest filed with the State Entity within ten (10) business days of receipt of final payment, shall release the State Entity and the State of Utah from all claims and all liability to the Contractor. The State Entity's payment for the Procurement Item(s) and/or services shall not be deemed an acceptance of the Procurement Item(s) and is without prejudice to any and all claims that the State Entity or the State of Utah may have against Contractor. The State of Utah and the State Entity will not allow the Contractor to charge end users electronic payment fees of any kind.
25. **INDEMNIFICATION RELATING TO INTELLECTUAL PROPERTY:** INTENTIONALLY DELETED
26. **OWNERSHIP IN INTELLECTUAL PROPERTY:** The State Entity and Contractor each recognizes that each has no right, title, or interest, proprietary or otherwise, in the intellectual property owned or licensed by the other, unless otherwise agreed upon by the parties in writing. All Procurement Item(s), documents, records, programs, data, articles, memoranda, and other materials not developed or licensed by Contractor prior to the execution of this Contract, but specifically manufactured under this Contract shall be considered work made for hire, and Contractor shall transfer any ownership claim to the State Entity. Contractor shall have the right to publish, upon prior written approval of the State Entity which may not unreasonably be withheld, the results of the project.
27. **OWNERSHIP IN CUSTOM DELIVERABLES:** INTENTIONALLY DELETED
28. **ASSIGNMENT:** Contractor may not assign, sell, transfer, subcontract or sublet rights, or delegate any right or obligation under this Contract, in whole or in part, without the prior written approval of the State Entity.
29. **REMEDIES:** Any of the following events will constitute cause for the State Entity to declare Contractor in default of this Contract: (i) Contractor's non-performance of its contractual requirements and obligations under this Contract; or (ii) Contractor's material breach of any term or condition of this Contract. The State Entity may issue a written notice of default providing a ten (10) day period in which Contractor will have an opportunity to cure. Time allowed for cure will not diminish or eliminate Contractor's liability for damages. If the default remains after Contractor has been provided the opportunity to cure, the State Entity may do one or more of the following: (i) exercise any remedy provided by law or equity; (ii) terminate this Contract; (iii) impose liquidated damages, if liquidated damages are listed in this Contract; (iv) debar/suspend Contractor from receiving future contracts from the State Entity or the State of Utah; or (v) demand a full refund of any payment that the State Entity has made to Contractor under this Contract for Procurement Item(s) that do not conform to this Contract.
30. **FORCE MAJEURE:** Neither party to this Contract will be held responsible for delay or default caused by fire, riot, act of God, and/or war which is beyond that party's reasonable control. The State Entity may terminate this Contract after determining such delay will prevent successful performance of this Contract.
31. **CONFIDENTIALITY:** If Contractor has access to or processes Confidential Information, Contractor shall: (i) advise its agents, officers, employees, partners, and Subcontractors of the obligations set forth in this Contract; (ii) keep all Confidential Information strictly confidential; and (iii) comply with any requirements contained in the contract regarding permitted uses and disclosures of personal data, measures designed to safeguard personal data, and the destruction of personal data. Contractor will promptly notify the State Entity of any potential or actual misuse or misappropriation of Confidential Information, including any data breaches, in accordance with UCA 63A-19 Government Data Privacy Act. In Accordance with UCA 63A-19, Contractor must comply with all the same requirements regarding personal data as the State.

Written Confidential Information shall be clearly marked as "confidential." If certain Confidential Information has not been reduced to written form at the time of disclosure by the State Entity, then such orally disclosed information shall be protected by the Contractor as Confidential Information, provided that the State Entity shall: (i) provide a statement to the Contractor that the oral information shall be protected under this Agreement; and (ii) within thirty (30) days of such disclosure, reduce to

writing a summary of the orally disclosed Confidential Information.

Contractor shall be responsible for any breach of this duty of confidentiality, including any required remedies and/or notifications under applicable law. Contractor shall indemnify, hold harmless, and defend the State Entity and the State of Utah, including anyone for whom the State Entity or the State of Utah is liable, from claims related to a breach of this duty of confidentiality, including any notification requirements, by Contractor or anyone for whom the Contractor is liable.

Upon termination or expiration of this Contract, Contractor will return all copies of Confidential Information to the State Entity or certify, in writing, that the Confidential Information has been destroyed. This duty of confidentiality shall be ongoing and survive the termination or expiration of this Contract.

32. **PUBLICITY:** Contractor shall submit to the State Entity for written approval all advertising and publicity matters relating to this Contract. It is within the State Entity's sole discretion whether to provide approval, which approval must be in writing.
33. **WORK ON STATE OF UTAH OR ELIGIBLE USER PREMISES:** Contractor shall ensure that personnel working on State of Utah premises shall: (i) abide by all of the rules, regulations, and policies of the premises; (ii) remain in authorized areas; (iii) follow all instructions; and (iv) be subject to a background check, prior to entering the premises. The State of Utah or Eligible User may remove any individual for a violation hereunder.
34. **CONTRACT INFORMATION:** INTENTIONALLY DELETED
35. **WAIVER:** A waiver of any right, power, or privilege shall not be construed as a waiver of any subsequent right, power, or privilege.
36. **SUSPENSION OF WORK:** Should circumstances arise which would cause the State Entity to suspend Contractor's responsibilities under this Contract, but not terminate this Contract, this will be done by formal written notice pursuant to the terms of this Contract. Contractor's responsibilities may be reinstated upon advance formal written notice from the State Entity.
37. **CHANGES IN SCOPE:** Any changes in the scope of the Procurement Item(s) to be performed under this Contract shall be in the form of a written amendment to this Contract, mutually agreed to and signed by both parties, specifying any such changes, fee adjustments, any adjustment in time of performance, or any other significant factors arising from the changes in the scope of the Procurement Item(s).
38. **PROCUREMENT ETHICS:** Contractor understands that a person who is interested in any way in the sale of any, Procurement Item(s), supplies, , construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, gratuity, contribution, loan, reward, or any promise thereof to any person acting as a procurement officer on behalf of the State of Utah, or to any person in any official capacity who participates in the procurement of such Procurement Item(s), supplies, , construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization.
39. **ATTORNEY'S FEES:** INTENTIONALLY DELETED
40. **TRAVEL COSTS:** If travel expenses are permitted by the Solicitation, then all travel costs associated with the delivery of Procurement Item(s) under this Contract will be paid according to the rules and per diem rates found in the Utah Administrative Code R25-7. Invoices containing travel costs outside of these rates will be returned to Contractor for correction.
41. **DISPUTE RESOLUTION:** INTENTIONALLY DELETED
42. **ORDER OF PRECEDENCE:** In the event of any conflict in the terms and conditions in this Contract, the order of precedence shall be: (i) this Attachment A; (ii) Contract Signature Page(s); (iii) the State of Utah's additional terms and conditions, if any; (iv) any other attachment listed on the Contract Signature Page(s); and (v) Contractor's terms and conditions that are attached to this Contract, if any. Any provision attempting to limit the liability of Contractor or limit the rights of the State Entity or the State of Utah must be in writing and attached to this Contract or it is rendered null and void.
43. **SURVIVAL OF TERMS:** Termination or expiration of this Contract shall not extinguish or prejudice the State Entity's right to enforce this Contract with respect to any default of this Contract or defect in the Procurement Item(s) that has not been cured, or of any of the following clauses, including: Governing Law and Venue, Laws and Regulations, Records Administration, Remedies, Dispute Resolution, Indemnity, Newly Manufactured, Indemnification Relating to Intellectual Property, Warranty of Procurement Item(s), Insurance.
44. **SEVERABILITY:** The invalidity or unenforceability of any provision, term, or condition of this Contract shall not affect the validity or enforceability of any other provision, term, or condition of this Contract, which shall remain in full force and effect.
45. **ERRORS AND OMISSIONS:** Contractor shall not take advantage of any errors and/or omissions in this Contract. The Contractor must promptly notify the State of any errors and/or omissions that are discovered.
46. **ENTIRE AGREEMENT:** This Contract constitutes the entire agreement between the parties and supersedes any and all other prior and contemporaneous agreements and understandings between the parties, whether oral or written.
47. **ANTI-BOYCOTT ACTIONS:** In accordance with Utah Code 63G-27 et seq., Contractor certifies that it is not currently engaged in any "economic boycott" nor a "boycott of the State of Israel" as those terms are defined in Section 63G-27-102. Contractor further certifies that it has read and understands 63G-27 et. seq., that it will not engage in any such boycott action during the term of this Contract, and that if it does, it shall promptly notify the State in writing.
48. **TIME IS OF THE ESSENCE:** The Procurement Item(s) shall be completed by any applicable deadline stated in this Contract. For all Procurement Item(s), time is of the essence. Contractor shall be liable for all reasonable damages to the State Entity, the State of Utah, and anyone for whom the State of Utah may be liable as a result of Contractor's failure to timely perform the Procurement Item(s) required under this Contract.
49. **PERFORMANCE EVALUATION:** The State Entity may conduct a performance evaluation of Contractor's Procurement Item(s), including Contractor's Subcontractors. Results of any evaluation may be made available to Contractor upon request.

50. **STANDARD OF CARE:** The Procurement Item(s) of Contractor and its Subcontractors shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having regular experience providing similar Procurement Item(s) which similarities include the type, magnitude, and complexity of the Procurement Item(s) that are the subject of this Contract. Contractor shall be liable to the State Entity and the State of Utah for claims, liabilities, additional burdens, penalties, damages, or third-party claims (e.g., another Contractor's claim against the State of Utah), to the extent caused by wrongful acts, errors, or omissions that do not meet this standard of care.
51. **REVIEWS:** The State Entity reserves the right to perform plan checks, plan reviews, other reviews, and/or comment upon the Procurement Item(s) of Contractor. Such reviews do not waive the requirement of Contractor to meet all of the terms and conditions of this Contract.
52. **Restricted Foreign Entities and Forced Labor:** In accordance with Utah law, Contractors contracting with the State certify that they are not providing a "forced labor product" as defined in Utah Code 63G-6a-121. If the Contractor is providing technology or technology services, networks, or systems, the Contractor certifies that the aforementioned does not come from a "restricted foreign entity," as also defined in UCA 63G-6a-121.

(Revision Date: 9/11/2025)

71.2229.000.000

Vendor # 08965

Kate Becker

From: Cole Selman <coleselman@utah.gov>
Sent: Wednesday, May 13, 2026 3:57 PM
To: a.toone@skinnytconstruction.com
Cc: geoff christensen; Kate Becker
Subject: Re: PDCF

CAUTION: This email originated from outside of Morgan County. Do not click links or open attachments unless you recognize the sender and know the content is safe. If you are unsure please contact Jeremy or Brandon.

Hey Adam,

Everything is good on our end. I think we were just waiting for the remaining money to fulfill the contract is all. If that has already been met then we can forward this over and get it processed. All looks good here. We'll get working on it

On Wed, May 13, 2026 at 12:56 PM <a.toone@skinnytconstruction.com> wrote:

Cole,

From the Morgan County treasurers records as reference, since the end of year 2024 through the year 2025 the county's predator control account has had a carryover balance of \$8,230.10 after paying the contract and collecting the Woolgrowers portion.
 Contrasting the year 2025 to 2026

	2025	2026
January 1 Balance	8,230.10	8,230.10
PDCF Contract amount	15,600	21,000
Date of Payment from Morgan County for contract	1/1/25	3/13/26
Woolgrowers match to Morgan County	7,800	2,000 + 8,050 + 450 = 10,500
Date of Woolgrowers match received	1/16/25	1/23/26 + 1/30/26 + 5/13/26
State of Utah match amount	7,800	00,000
State of Utah match amount Date Received	1/27/25	--/--/-- ?

The 10,050 from the Woolgrowers and the carryover balance from 2025 were used to make an 18,280.10 portion of the payment made on 3/12/26. The remaining 2,719.90 balance needed to fulfill the contract was discretionarily pulled from Kate's, County manager, account.

The woolgrowers have made an additional payment of \$450 to the county treasurer today fulfilling the matching obligation for 2026. I apologize for my math error.

MORGAN COUNTY
REQUEST FOR PAYMENT

VENDOR NAME: PDCF (Vendor # 28965)

ADDRESS: _____

INVOICE # Agreement 83870FB INVOICE DATE: _____

ACCOUNT # _____ PAYMENT DUE DATE: _____

DESCRIPTION: FY 2026-2027 Agreement

AMOUNT DUE: 21,100 GL ACCOUNT: 71-2229-000-000

GL ACTIVITY CODE (GRANT): _____

EXPLANATION OF PURCHASE: ~~Budget Adjustment Submitted~~ See budget adjustment

APPROVED BY: _____

DATE: _____

Department Head

County Auditor

REJECTED FOR:

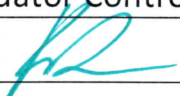
_____ INCOMPLETE FORM

_____ OVER BUDGET

_____ MISSING DOCUMENTATION



2026 BUDGET CHANGE FORM

Date	08/11/2026
Department	Predator Control
Department Head Signature	
	Kate Becker
Amount	9,700
Move from GL Account#	71-2229-000-000
Move to GL Account #	71-2229-000-000

Brief Description

The woolgrowers will be paying the county \$10,550 for predator control. We have \$11,400 in the account but need to increase the budget by \$9,700 to cover the pass through \$21,100 check.

Clerk/Auditor Use Only

Date Entered:
Date Commission Approved:



2026 UAC ANNUAL CONVENTION

SEPTEMBER 8-10, 2026

UTAH VALLEY CONVENTION CENTER

PROVO, UT

The UAC Annual Convention in the fall is the largest meeting of county elected and appointed officials in the state of Utah. Participants from all counties are invited to come together to shape UAC's policy agenda, share proven practices and strengthen knowledge networks to help improve residents' lives and efficiency of county government.

Tuesday, September 8, 2026 - Evening UAC Board Meeting

Wednesday, September 9, 2026

8:00am - 5:00pm - Affiliate Breakouts, Exhibitor Time, Meals

5:00pm - Attendee Dinner/County Basket Giveaway

Thursday, September 10, 2026

8:00am - 3:00pm - Affiliate Breakouts, Exhibitor Time, Meals

USACCC Conference

Registration
Available Soon

 Nov 18, 2026 — Nov 20, 2026

 Little America & Utah
Association of Counties, Salt
Lake County, UT

Laura Barlow

(801) 201-3813

laura@utahcounties.org