Services Guide

This Services Guide contains provisions that define, clarify, and govern the services described in the quote (the "Quote") provided to you by EMD Networking Services, Inc. It expands upon the service descriptions in the Quote and should be read together with the Quote and the Master Services Agreement. Services and coverage vary by plan. If the Quote conflicts with a generalized description in this Guide, the more specific scope stated in the Quote controls.

Plan Levels

Essential

Purpose: A professional and secure technology foundation for small businesses that need dependable protection, proactive maintenance, and help with common unexpected issues, but do not require EMD to serve as their complete day-to-day IT department.

Backups: Secure image-based backups for covered systems, with up to 30 days of retention, one recovery point per day, and 1 TB of included cloud storage. Supported firewall configurations are backed up. File-based backup, BDR hardware, and BDR support are not included unless separately quoted.

Security and maintenance: Includes 24/7 managed endpoint threat monitoring, investigation and containment; critical operating-system security patching; automated system-health monitoring and remediation; and automated hardware and software inventory.

Labor: Includes remote troubleshooting and corrective labor intended to restore existing, covered technology that unexpectedly stops working or no longer operates as previously configured. Coverage is limited to attempting to return the affected technology to its prior working condition. New installations, additions, moves, changes, upgrades, reconfiguration, user or device setup, onboarding or offboarding, training, routine administration, optimization, vendor coordination, onsite work, after-hours work, projects, and unsupported technology are billed separately at a 20% discounted labor rate. Emergency response is best effort.

Managed

Purpose: A comprehensive service plan in which EMD functions as the Customer's day-to-day IT department. The Managed plan includes everything in the Essential plan and adds broad remote and onsite support, stronger cybersecurity administration, enhanced backup capability, and routine coordination of supported technology.

Backups: Image and file-based backups with up to 60 days of retention, up to six recovery points per day, 5 TB of included cloud storage, and Basic BDR Support when compatible BDR hardware is present. BDR hardware is additional unless expressly included in the Quote.

Security and maintenance: Adds managed threat remediation and security review, third-party application patching, manual investigation and remediation of failed patches, network-based DNS filtering, 24/7 managed identity threat monitoring, investigation, and containment, including risky users and risky sign-ins, email-authentication and domain-protection review with configuration updates, annual user-access and environment reviews, managed endpoint privilege control, 30-day firewall log retention, managed network-device configuration backups, and ongoing administration of supported Microsoft 365 or Google Workspace settings.

Labor: Includes unlimited remote and onsite labor for normal daily IT needs, including reactive and proactive requests, user onboarding and offboarding, workstation setup, routine software and device administration, connectivity troubleshooting, and first-line vendor coordination. Response labor is included for up to two qualifying after-hours emergencies per month. Emergency priority response is two business hours or less. Project and other out-of-scope labor is discounted 40%.

Advanced

Purpose: EMD's highest service level for organizations that want comprehensive daily support plus advanced security, resilience, governance, reporting, and executive technology leadership. The Advanced plan includes everything in the Managed plan and adds deeper analysis, more frequent review, and proactive planning intended to reduce risk and improve long-term technology decisions.

Backups: Image and file-based backups with up to 365 days of retention, up to 24 recovery points per day, 10 TB of included cloud storage, and Advanced BDR Support when compatible BDR hardware is present. BDR hardware is additional unless expressly included in the Quote.

Security, governance, and planning: Adds centralized collection and monitoring of supported security logs, ongoing vulnerability scanning and remediation coordination, advanced endpoint and identity reporting, post-incident analysis, advanced email authentication and domain protection, cloud and mobile-device management, privilege-policy review and optimization, monthly patch-compliance and health reporting, capacity and lifecycle forecasting, semiannual security and technology reviews, risk analysis, budget planning, architectural guidance, roadmap integration, and device-based DNS and web protection with off-network filtering and enhanced reporting.

Labor: Includes the broad daily IT support included with the Managed plan, plus priority incident coordination, defined response labor, post-incident reporting, enhanced vendor and compliance support, and more advanced cloud administration. Response labor is included for up to four qualifying after-hours emergencies per month. Emergency priority response is one business hour or less. Out-of-scope project labor is discounted 50%.

Core Services & Benefits

Managed Endpoint Detection & Response (EDR)

Provides a business-class endpoint detection and response platform on covered workstations and servers, with continuous monitoring for suspicious behavior, malware, ransomware, and other threats. Services may include 24/7 detection, investigation, automated or analyst-directed containment, EMD remediation and review of routine alerts, deeper reporting, system and policy optimization, and post-incident analysis, as specified in the Quote. No security platform can prevent every event, and coverage depends on a healthy installed agent, supported operating system, internet connectivity, and user compliance with security requirements.

Managed Identity Threat Detection & Response (ITDR)

Continuously monitors supported cloud identities for activity that may indicate compromised credentials, malicious sign-ins, privilege abuse, or account takeover. Services may include 24/7 investigation and containment of supported identity threats, identity-security reviews, remediation recommendations, policy optimization, expanded reporting, post-incident analysis, and review of licensing or configuration gaps that may reduce protection, as specified in the Quote. Available actions depend on the Customer's cloud platform, licensing, administrative access, and the controls supported by that environment.

Proactive System Health Monitoring & Remediation

Continuously monitors covered systems for availability, service failures, storage capacity, performance conditions, and other indicators of declining health. Automated routines attempt to correct common conditions before they cause disruption. Services may also include manual remediation labor when an eligible alert cannot be corrected automatically, monthly reporting, capacity trends, recurring-problem analysis, and lifecycle recommendations, as specified in the Quote. Rapid failures can occur before an alert is received or acted upon; monitoring is a risk-reduction service and does not guarantee uninterrupted operation.

OS & Application Patch Management

EMD configures and monitors deployment of critical operating-system security patches to covered devices. Services may also include supported third-party application patching, labor to investigate and remediate failed patch installations, monthly compliance reporting, exception review, and policy optimization, as specified in the Quote. Patches are created and tested by third-party vendors; EMD may defer a release when a known compatibility or stability concern exists. Some devices may require restarts, adequate free space, internet connectivity, and regular powered-on time. EMD is not responsible for vendor defects or incompatibilities caused by a released update.

Firewall & Internet Availability Monitoring

Monitors supported firewalls and primary internet connections for availability and outage conditions. Services may also include troubleshooting and restoration labor for covered connectivity failures, traffic and performance analysis, reporting, and capacity recommendations, as specified in the Quote and subject to provider and equipment limitations. Internet service levels, carrier repair times, circuit replacement, cabling, electrical service, and third-party fees remain outside EMD's control and are not guaranteed by this service.

Technology Asset Inventory & Lifecycle Management

Maintains an automated inventory of covered hardware and software to improve visibility, support licensing and standards reviews, and help identify aging or unsupported technology. Services may also include periodic lifecycle review, reporting, replacement recommendations, formal technology standards, refresh forecasting, budget planning, and roadmap integration, as specified in the Quote. Inventory accuracy depends on active management agents, network visibility, vendor data, and Customer disclosure; equipment not connected or not covered may not appear.

Managed Network Infrastructure

Provides ongoing administration of supported switches, wireless access points, firewalls, VPNs, and related network services. Services may include secure configuration backups, routine support for covered equipment, periodic configuration and architecture reviews, performance and traffic analysis, capacity recommendations, and planning intended to improve security, reliability, scalability, and recoverability, as specified in the Quote. Equipment must be supported, properly licensed, and under an active manufacturer subscription when required.

Managed Remote Access

Provides covered users with secure remote access to supported workstations and approved resources from offsite locations. EMD installs, configures, and maintains the supported remote-access platform and assists with ordinary connection issues. Access is limited to authorized users and devices and may require multifactor authentication, compatible endpoint protection, and qualifying cloud or security licenses. This service does not include access to unsupported personal devices, bypassing Customer security policies, or remediation of the user's home internet or personal network.

Emergency Priority Response

Critical incidents that materially interrupt business operations receive priority handling when reported by telephone and identified as an emergency. The applicable initial response target and coverage terms are stated in the Quote. A response means acknowledgement and commencement of triage, not guaranteed resolution. Restoration time depends on the nature of the failure, vendor availability, replacement equipment, access, and other factors outside EMD's control.

Emergency Loaner Equipment

EMD maintains a limited pool of temporary equipment intended to reduce downtime following certain critical hardware failures. Access, included setup and deployment labor, and any applicable charges are determined by the coverage stated in the Quote. Loaners remain EMD property, are provided temporarily, may not match the failed equipment, and must be returned promptly when permanent equipment is restored or installed. Specialized hardware, licensing, freight, data recovery, and replacement equipment are not included unless stated in the Quote.

Managed Backup, Recovery & Business Continuity

Provides secure image-based and, where applicable, file-based backup of covered systems. Backup frequency, retention, included cloud storage, BDR Support, and other recovery features are stated in the Quote. BDR hardware and extra storage are additional unless expressly included. Only selected data and covered devices are protected; successful backups and restore testing reduce risk but do not guarantee recovery from every event.

Labor-Inclusive Services

Remote Help Desk Support

Remote technical assistance for covered users and devices may include common reactive break/fix incidents, such as password resets, email and application-access problems, software errors, and virus or malware remediation. The Essential plan provides some coverage only for unexpected problems affecting existing, covered technology, with the goal of restoring its prior working condition. Select plans add unlimited reactive and proactive remote labor for normal daily IT needs. 'Unlimited' is subject to reasonable use and the defined scope and excludes projects, unsupported systems, training, development, data entry, and other expressly excluded work.

On-site Support

In-person technical assistance when an eligible issue cannot be effectively resolved remotely, including covered hardware troubleshooting, workstation setup, and routine connectivity or equipment support. Whether onsite labor is included or separately billed is determined by the coverage stated in the Quote. Travel outside the normal service area, project work, specialized cabling, physical construction, equipment relocation, and third-party charges are excluded unless quoted.

User & Device Administration

Routine administration of supported users, accounts, access, software, and devices. Typical work includes onboarding and offboarding, account and password changes, access updates, standard software installation and configuration, workstation setup, printer mapping, and ordinary device changes. Whether this labor is included or separately billed is determined by the Quote. Licensing, hardware, large deployments, migrations, and significant configuration changes are projects or separately billed work.

Mobile/Shared Device Management

Management of supported shared, kiosk, dedicated-purpose, or similar devices that are not associated with a normally managed user. Services may include routine enrollment, configuration, policy administration, and device onboarding or offboarding, as stated in the Quote. Applicable Microsoft or other software licensing is additional. Initial buildout, enrollment profiles, policies, applications, or significant changes may require a separately quoted project.

Third-Party Technology Support & Vendor Coordination

Provides first-line troubleshooting and routine coordination with vendors of supported business technology, such as internet providers, line-of-business applications, printers, security systems, and communications platforms. EMD will gather relevant technical details, help isolate whether the issue is within the managed environment, open or participate in vendor cases, and assist with reasonable follow-through. Services may also include recurring-issue review, vendor-performance discussion during technology planning, and reasonable assistance with third-party technical compliance requests, as specified in the Quote. Vendor fees and work outside EMD's control are not included.

After-Hours Emergency Support

Technical response outside EMD's normal business hours for qualifying emergencies that significantly disrupt operations or affect a critical covered system. Included incident allowances and applicable after-hours charges are stated in the Quote. Incidents beyond any allowance are billed at the applicable after-hours rate, and holiday work may be billed at double-time rates. The Customer must telephone EMD and follow the emergency prompts; email or portal submission alone does not activate emergency handling.

IP Camera Support

Limited technical support for supported IP camera systems connected to the Customer's managed network may include connectivity and network troubleshooting and vendor coordination, as specified in the Quote. Physical connections, mounting, aiming, cleaning, cabling, electrical work, replacement, surveillance monitoring, footage

review, retention assurance, and manufacturer subscription costs are excluded. Labor not included in the Quote is billed separately.

VoIP Communications / Phone Support (non-EMD VoIP)

Limited support for third-party VoIP systems may include network connectivity troubleshooting, minor configuration changes, and coordination with the Customer's phone vendor, as specified in the Quote. Provider outages, carrier configuration, number porting, handsets, licenses, subscriptions, and vendor charges are not included. More extensive administration may require a separate VoIP support service or project, and labor not included in the Quote is billed separately.

Labor Discounts for Out-of-Scope Services

Approved project and out-of-scope labor may be discounted from EMD's then-current standard rates as stated in the Quote. A project generally involves a new system, major addition, migration, deployment, redesign, office move, large-scale refresh, or substantial change to the existing environment. Projects are quoted and approved before work begins. Discounts apply only to eligible EMD labor and do not apply to hardware, software, licensing, subscriptions, freight, taxes, or third-party charges unless expressly stated.

Security Services

Virus & Malware Remediation

Includes investigation, containment, and remediation of detected viruses and malware on covered systems. Services may include ordinary virus and malware remediation associated with covered reactive support, broader managed remediation and review, and coordinated remediation of identified Common Vulnerabilities and Exposures (CVEs) and related weaknesses on supported systems when a supported correction is available, as specified in the Quote. Major incident recovery, forensic investigation, legal or regulatory response, rebuilding systems, and remediation of unsupported technology may be separately billed.

Cybersecurity Incident Response Support

Provides initial investigation, containment coordination, and basic remediation for suspected cybersecurity events affecting covered systems. Services may include investigation and remediation of routine incidents, priority coordination, defined response labor, and a post-incident report appropriate to the event, as specified in the Quote. The service is not cyber insurance, a guarantee against compromise, or a substitute for specialized legal, forensic, breach-notification, public-relations, or compliance services. Significant incidents may require a separately approved response project or outside specialist.

Microsoft 365 & Google Workspace Administration

Provides administration of supported identities, email, collaboration tools, and available security settings within the Customer's cloud environment. Services may include ongoing routine administration of users, email, collaboration, and supported security settings, as well as security optimization, governance, reporting, and deeper policy management, as specified in the Quote. Licensing is not included and EMD will recommend the level needed for selected controls. Capabilities unavailable under the Customer's licenses cannot be implemented or guaranteed.

User Access & Permissions Review

Reviews active users, administrative roles, access rights, and selected permissions to identify unnecessary, excessive, or risky access. The review frequency and included services, which may include findings, remediation planning, privileged-access governance, and licensed automation, are stated in the Quote. Reviews are point-in-time and rely on access to the systems and data included in scope. Remediation that constitutes a migration, redesign, or large-scale permissions project may be separately quoted.

Network Health Best-Practice Review

Evaluates the supported IT environment against EMD standards and generally accepted security, reliability, supportability, and lifecycle practices. The review frequency and included services, which may include findings, prioritized recommendations, risk analysis, and integration into the Customer's technology roadmap and budget planning, are stated in the Quote. The review is advisory, is not an audit or certification, and does not guarantee compliance with a particular legal, insurance, or industry requirement.

Network Device Configuration Backup

Securely retains configuration backups for supported network equipment so settings can be restored more efficiently if a device fails, is reset, or is changed unexpectedly. Covered equipment and any included configuration review for security, stability, and performance are stated in the Quote. Backup capability varies by manufacturer, model, licensing, and management platform. Replacement hardware, vendor subscriptions, and reconstruction of unsupported configurations are not included.

Centralized Security Logging & Threat Monitoring (SIEM)

Provides retention, centralized collection, and monitoring of supported security logs to assist with correlation, detection, investigation, and incident review, as specified in the Quote. Sources, event volume, retention, and available detections depend on supported integrations and licensing. The service does not guarantee that every

malicious action will generate a useful log or alert, and it is not a replacement for legal-grade forensic preservation unless specifically quoted.

Managed Vulnerability Assessment & Remediation Coordination

Performs ongoing scanning of supported systems to identify known vulnerabilities and security weaknesses. Findings are validated where practical, prioritized according to risk and business context, reported, and tracked through remediation. EMD coordinates supported patches, configuration changes, or mitigation steps within the scope stated in the Quote. Vendor fixes, application upgrades, replacement of obsolete equipment, business-risk acceptance, penetration testing, and major remediation projects may require separate approval and charges.

Risky Users & Risky Sign-ins

Monitors supported identity alerts that may indicate compromised credentials, impossible travel, suspicious sign-in behavior, leaked credentials, or other account risk. Services may include active investigation and containment when the available platform produces a qualifying alert, deeper identity-risk analysis, trend review, and recommendations to strengthen policy and reduce repeat exposure, as specified in the Quote. Effectiveness depends on qualifying licenses, accurate user information, enabled logging, and supported identity controls.

Privileged Access Management (PAM) & Privileged Identity Management (PIM)

Removes standing local administrator rights from covered users and provides a controlled method for temporary privilege elevation through approved requests or rules. Select plans may also include privileged identity management for administrative roles, policy review, reporting, optimization, and advanced configurations, as specified in the Quote and subject to applicable licensing. These controls reduce risk but do not guarantee approval of every application or workflow. Unsupported applications that require permanent administrator access may need to be replaced or excepted at the Customer's risk.

Email Authentication & Domain Protection

Provides configuration and management of SPF, DKIM, and DMARC for supported email domains to reduce spoofing and improve message authentication. Services may include a baseline review, configuration updates, ongoing monitoring, policy optimization, deliverability reporting, and coordinated updates as authorized senders change, as specified in the Quote. Results depend on control of DNS, accurate identification of sending services, and cooperation from third-party platforms. Authentication reduces impersonation risk but does not prevent all phishing, look-alike domains, compromised accounts, or delivery problems.

Cloud & Mobile Device Management

Provides centralized management of supported computers, smartphones, tablets, and cloud-only devices. EMD applies approved settings, security policies, application controls, compliance rules, and access requirements to help protect company information and maintain consistent configuration. Capabilities vary by operating system, ownership model, manufacturer, cloud platform, and license. Enrollment may affect privacy and permitted use of managed devices; the Customer is responsible for communicating its policies and obtaining any required employee consent.

Managed DNS & Web Threat Protection

Protects users from malicious websites, phishing, and unsafe online content through DNS security and web filtering. Coverage may include network-based DNS filtering and, where specified in the Quote, device-based protection for users away from the managed network, along with enhanced reporting. Effectiveness depends on supported devices, active agents or network configuration, internet connectivity, and applicable licensing. No filtering service can identify or block every harmful or inappropriate destination.

Optional Services

Workforce Productivity

Provides workforce analytics and employee-activity monitoring to help authorized managers understand how technology is used during the workday. The platform may record application and website usage, active and idle time, work patterns, trends, and other configured activity indicators, then present dashboards and reports for operational analysis. EMD assists with deployment and routine administration of the service; the Customer determines permitted users, policies, communications, and employment decisions. The Customer is solely responsible for providing required notice, obtaining consent, limiting access, and using the information in accordance with applicable employment, privacy, labor, and monitoring laws. A minimum of five users is required.

Advanced Password Manager

Provides a centralized, encrypted vault for users to create, store, retrieve, and share business passwords and other sensitive credentials. Features may include strong-password generation, controlled sharing, browser and mobile access, group permissions, audit information, and administrative recovery. EMD configures the organization and provides ordinary administration, but users remain responsible for protecting their master credentials and multifactor authentication methods. The service reduces risks associated with weak, reused, or informally shared passwords but cannot prevent misuse by an authorized user or compromise of an unlocked device.

Security Awareness Training (SAT)

Provides ongoing employee education and simulated phishing exercises designed to help users recognize phishing, social engineering, malicious links, credential requests, and other common threats. Training content and campaign timing may be adjusted based on results and emerging risks. Reporting helps authorized Customer contacts identify participation and recurring areas of concern. The service reduces human risk but cannot guarantee that a user will identify or avoid every threat. The Customer is responsible for employee participation, internal policy enforcement, and any employment actions based on results.

Managed Email Signatures

Centrally creates and applies standardized email signatures, contact details, branding, disclaimers, and approved messaging across supported Microsoft 365 users. Central management reduces inconsistent formatting and avoids reliance on each user to update a local signature. EMD performs ordinary template and user-detail administration using information supplied by the Customer. Complex graphic design, frequent campaign changes, non-supported mail platforms, and custom integrations may be separately billed. A minimum of ten licenses applies, generally based on the number of covered cloud users.

EMD VoIP Communications

Provides a hosted business telephone platform with calling, voicemail, automated attendants, call routing, mobile and desktop applications, and other selected communications features. Users can communicate from the office, home, or while traveling while maintaining a consistent business identity. EMD provides a customized proposal based on users, numbers, devices, calling requirements, locations, and desired features. Internet service, electrical power, emergency-calling location information, number portability, taxes, regulatory charges, equipment, and term commitments are addressed in the separate VoIP quote and service terms.

Licensing and prerequisites: Microsoft 365 and Google Workspace licensing is not included in service-plan pricing unless expressly listed in the Quote. EMD will recommend licensing based on the selected plan and desired capabilities. If required licensing, supported hardware, administrative access, internet connectivity, or manufacturer subscriptions are not acquired or maintained, affected services may be limited or unavailable. Certain features require a business-class router with an active subscription. Local backups require a compatible local storage device, which will be quoted if the Customer does not already have one.

Assumptions / Minimum Requirements / Exclusions

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements:

- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software, or if our Services begin prior to you licensing supported versions of Microsoft Windows®, then you agree that within 90 days after Services begin, you will update to a current version on the Covered Hardware or replace the applicable devices with equipment that comply with this paragraph.
- All software must be genuine, licensed and vendor-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The Environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the environment must be securely encrypted.
- An outside static IP address may be required for some remote access solutions and we highly recommend one for those types of services.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Customer must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Customer must provide us with exclusive administrative privileges to the Environment.
- Customer must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

Exclusions. Services that are not expressly described in the Quote will be out of scope and will not be provided to Customer unless otherwise agreed, in writing, by EMD. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by EMD in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the Environment up to the Minimum Requirements (unless otherwise noted in “Scope of Services” above).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels

Automated monitoring is provided on an ongoing (i.e., 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-TH, 8AM-5PM, FRI 7AM-4PM Pacific Time, excluding legal holidays and EMD-observed holidays listed below), unless otherwise specifically stated in the Quote or described below.

If the Quote indicates that you receive the Advanced plan: We will respond to emergency or critical issues (defined as situations in which all or practically all of an entire managed network is affected) within one (1) business hour after being notified of the applicable issue.* All other issues will be handled on a best-efforts basis and are subject to technician availability.

If the Quote indicates that you receive the Managed plan: We will respond to emergency or critical issues (defined as situations in which all or practically all of an entire managed network is affected) within two (2) business hours after being notified of the applicable issue.* All other issues will be handled on a best-efforts basis and are subject to technician availability.

* All emergency/critical response time frames are calculated from the time EMD is notified by Customer by telephone at a main office number and through the dispatcher. Notice in another manner may delay remediation. Emailing or calling a technician directly is not acceptable and may delay our response.

Technical support under the Essential plan and any service level other than the Advanced or Managed plan is provided on a best-efforts basis and is subject to technician availability.

Support During Off-Hours/Non-Business Hours: The Advanced plan includes response labor for up to four (4) qualifying after-hours incidents per month, and the Managed plan includes response labor for up to two (2) qualifying after-hours incidents per month. Other off-hours support is offered case by case, subject to technician availability, and billed at then-current overtime rates, and double-time rates during holidays, unless the Quote expressly states otherwise.

All remote hourly services are billed in 15-minute increments, with partial increments rounded to the next highest increment. On-site hourly services have a one (1) hour minimum, and a one (1) hour minimum applies to all Non-Business Hour Support as well.

EMD-Observed Holidays: EMD is closed for the following holidays, if they fall on a regular work day. If they fall on a non-work day they may be 'observed' on a day other than the date of the holiday:

- New Year's Day
- Good Friday – Half Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Day

Service Credits: Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Customer timely brings that failure to our attention in writing (as per the requirements of the MSA), then Customer will be entitled to receive a pro-rated service credit equal to 1/30 of

that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

Auditing Services

We will audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services are comprised of:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software
- Security vulnerability check
- Backup and disaster recovery solution audit
- Speed test and ISP audit
- Office phone vendor service audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

Onboarding Services

If onboarding services are provided under the Quote, then the following services will be provided to you.

- Secure network by changing passwords for admins, user accounts, routers, switches, email accounts, ILO access, VPN's, etc. using secure password formats.
- Uninstall any monitoring tools or other software installed by previous IT consultants.
- Determine existing backup strategy and status; prepare backup options for consideration and get backups scheduled asap.
- Redirect local folders so data gets saved to proper locations to be backed up.
- If the Quote includes Managed Email, prepare and schedule backups of MS365 accounts asap.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and RMM agents and install our managed antivirus application and RMM agents.
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup, antivirus, and spyware scans.
- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on all devices.
- Stabilize network and assure that all devices can securely access the file server.
- Review and document current server configuration and status.
- Review password policies and update user and device passwords.
- Review group policy settings and make changes as needed.
- Review and setup printers properly for best practices.
- Gather and document all SSL certs, domains and other registrations to manage renewals.
- Distribute instructions on requesting service, dispatch guidelines, etc to end users.
- As applicable, make recommendations for changes that should be considered to the managed environment.
- More (over 90 total items in our complete on-boarding task list)

The foregoing list is subject to change if we determine, in our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.

Ongoing / Recurring Services

Ongoing/recurring services are services that are provided to you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Ongoing services generally begin upon the completion of on-boarding services; therefore, any delays or interruptions to the onboarding services may delay the commencement of ongoing/recurring services.

Fees

The fees for the Services will be as indicated in the Quote. Recurring services are billed in advance for the upcoming calendar month, and payment is due within thirty (30) days of the invoice date.

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Pricing is based on factors including Customer locations, servers, workstations, cloud users, backup storage requirements, and other covered equipment. If the managed environment, quantities, or requirements change, you agree that monthly fees may be adjusted accordingly.

Annual Increases. To account for increases in service, licensing, and labor costs, pricing will increase by an average of three percent (3%) to five percent (5%) on each annual anniversary of the Agreement. We also reserve the right to increase monthly recurring fees and data recovery-related fees. If an increase exceeds five percent (5%) of the fees charged for the Services in the prior calendar year, you will have sixty (60) days to terminate the Services by written notice. You remain responsible for fees accrued through termination and all pre-approved, non-mitigatable expenses. Continued use after that period indicates acceptance of the increase.

Pass-Through Increases. We reserve the right to pass through increases in costs or fees charged by third-party providers. Because we do not control those providers, we cannot predict whether increases will occur, but we will endeavor to provide as much advance notice as reasonably possible.

Travel Time. If onsite services are provided, travel within city limits is at no charge. Travel outside city limits is billed at then-current hourly rates, plus tolls, parking, and related expenses. If you have a current Managed or Advanced agreement, onsite travel is at no charge unless you request additional visits not required for normal servicing of the account.

Appointment Cancellations. You may cancel or reschedule at no charge with at least one business day's notice. If timely notice is not received, you are not present, or we are denied access at the scheduled time, you agree to a cancellation fee equal to two (2) hours at the applicable current consulting rate.

Automated Payment. For recurring services, ACH Auto Pay through our payment portal is required. Payment-method requirements and applicable fees are described on the following page.

All recurring monthly invoices must be paid through ACH Auto Pay using EMD's payment portal at portal.emdnet.com. Customer must enroll in and maintain ACH Auto Pay. A $35 monthly processing fee applies if Customer does not enroll in, maintain, or pay through ACH Auto Pay. Credit cards are not accepted for recurring service payments.

ACH. When enrolled in ACH payment processing, you authorize us to electronically debit the checking or savings account designated in the payment portal for amounts due under the Quote. This authorization continues until terminated in writing. A $35 service charge applies to an electronic debit returned unpaid because of insufficient funds or bank restrictions.

Credit Card. Credit cards may be used only for eligible non-recurring invoices under $1,000. Invoices of $1,000 or more and all recurring monthly fees must be paid by ACH or, where permitted, check. Recurring service fees may not be paid by credit card.

Check. Where EMD permits payment by check, the check must be delivered before Services commence. Returned, incorrect, incomplete, or insufficient-funds checks are subject to a $50 administration fee plus applicable bank charges. The $35 monthly processing fee above applies to recurring invoices not paid through ACH Auto Pay.

Microsoft Licensing Fees. The Services may require per-seat Microsoft New Commerce Experience (NCE) Licenses for Microsoft 365, Dynamics 365, Windows 365, or Microsoft Power Platform. NCE Licenses cannot be canceled after purchase or transferred to another customer and may require a one- or three-year term. Regardless of why Services terminate, you must pay all applicable NCE Licenses in full for their entire terms. If paid in full, you may use the licenses until they expire, even if you move to another managed service provider.

Labor Rate Discounts. Discounts for projects or other out-of-scope work are stated in the Quote and apply to eligible EMD labor only. They are calculated from EMD's then-current standard labor rates, which may change. Current labor rates are available at https://emdnet.com/rates.

Minimum Initial Term and Termination. The minimum initial term is six (6) months for the Essential and Managed plans and nine (9) months for the Advanced plan. If project discounts were contingent on activating an Agreement, the minimum initial term is one (1) year regardless of plan. EMD may terminate with thirty (30) days' written notice. Customer may terminate with thirty (30) days' written notice after completing the applicable minimum initial term.

Requesting Service

All standard service requests must be submitted through the Customer portal or by emailing help@emdnet.com. This ensures that a ticket is created, placed in the service queue, and prioritized appropriately for the fastest possible response. Use one of the following methods:

- **Email:** Send help@emdnet.com a brief description in the subject line and useful details in the message body so the correct resource can be scheduled and prepared.
- **Customer portal:** Create a new ticket at portal.emdnet.com.

If you are unable to access the Customer portal or email, call one of our main phone lines at 559-636-7000 or 805-439-1055 and follow the prompts. Do not contact a technician or other EMD employee directly; doing so may delay the response because technicians cannot schedule themselves and may not receive direct messages promptly.

For emergency service requests, always call a main phone line and identify the request as an emergency. Emergency requests should be limited to situations in which all or the majority of the managed environment is down or severely limited.

For after-hours service requests, call a main phone line and follow the prompts. Someone will contact you as soon as possible. Unless the Quote includes after-hours support, service is billed at normal overtime rates with a one-hour minimum.

Removal of Software Agents

Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the Environment. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the Environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, Customer will remove, package and ship, at Customer's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Customer by EMD that were used in the provision of the Services. If you fail to timely return all equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Additional Terms

Authenticity

Everything in the managed environment must be genuine and licensed—including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by EMD, and Customer shall not modify these levels without our prior written consent.

Remediation

Unless otherwise provided in the Quote, remediation services will be provided in accordance with the recommended practices of the managed services industry. Customer understands and agrees that remediation services are not intended to be, and will not be, a warranty or guarantee of the functionality of the Environment, or a service plan for the repair of any particular piece of managed hardware or software.

Network Security & Access

Administrative access to the network and related systems will be limited to authorized EMD personnel during the Agreement unless EMD approves otherwise in writing. No other IT provider, user, or third-party vendor may add, remove, or modify user accounts, hardware, software, services, or system configurations related to IT support without EMD's prior written approval. Any approved hardware or technology must be incorporated into and governed by the Agreement. Unauthorized changes may disrupt the Services, reduce security, or increase third-party charges, and Customer is responsible for resulting costs.

Modification of Environment

Changes made to the Environment without our prior written approval or knowledge may substantially and negatively affect the Services and may change the fees charged under the Quote. You agree not to move, modify, add, remove, install, or otherwise alter any portion of the Environment without our prior written approval. This includes hardware, applications, accounts, services, configurations, and log files. Work required to diagnose or correct problems arising from unauthorized changes is outside scope unless EMD agrees otherwise in writing.

Co-Managed Environment

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by us), we will endeavor to implement the Services an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention.

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. In order to improve security awareness, you agree that EMD or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data impacted by the incident will be recoverable. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Customer's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the Environment, or (ii) prevents normal access to the Environment, or impedes or disrupts the normal functions of the Environment.

Environmental Factors

Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances.

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all Services that are described or designated as "unlimited." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (e.g., requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email"). Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting

any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by EMD or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. EMD reserves the right, but not the obligation, to suspend Customer's access to the Hosted Email and/or all transactions occurring under Customer's Hosted Email account(s) if EMD believes, in its discretion, that Customer's email account(s) is/are being used in an improper or illegal manner.

Patch Management

We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Customer's data. Neither EMD nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. EMD cannot and does not warrant that data corruption or loss will be avoided, and Customer agrees that EMD shall be held harmless if such data corruption or loss occurs. Customer is strongly advised to keep a local backup of all of stored data to mitigate against the unintentional loss of data.

Procurement

Equipment and software procured by EMD on Customer's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Customer to the greatest extent possible. By procuring equipment or software for Customer, EMD does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Customer's responsibility in the event that a return of the Procured Equipment is requested. EMD is not a warranty service or repair center. EMD will facilitate the return or warranty repair of Procured Equipment; however, Customer understands and agrees that (i) the return or warranty repair of Procured Equipment is

governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which EMD will be held harmless, and (ii) EMD is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier. If equipment is purchased through EMD, we will handle the processing of any warranty claims, shipping the product back to the vendor (if applicable) and receiving the product back from the vendor and testing before putting it back into the Environment. Because of this service, EMD may not be able to match or be comparable to pricing you may be able to obtain elsewhere or on your own. If equipment is purchased by you directly (not through EMD) you will be responsible for the processing of any warranty claims, shipping the product and receiving it and testing before it is put back into the Environment.

Best Practice Reviews/Heath Assessments; IT Strategic Planning

Suggestions and advice rendered to Customer are provided in accordance with relevant industry practices, based on Customer's specific needs and EMD's opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, EMD is not endorsing any particular manufacturer or service provider.

Penetration Testing; Vulnerability Assessment

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing process, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees or expenses arising or resulting from (i) any response to the penetration testing services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity is not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

Obsolescence

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires "end of support" status from the applicable device's or software's manufacturer ("Obsolete Element"), then we may designate the device or software as "unsupported" or "non-standard" and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our "best efforts" only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element, (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose), or (iii) remove the Obsolete Element from the Environment so it does not risk the security of the rest of the Environment. If you are not agreeable to any of these options we may elect to cancel Services to avoid risk or liability of the Environment's security. In any event, we

make no representation or warranty whatsoever regarding any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

Hosting Services

You agree that you are responsible for the actions and behaviors of your users of the Services. In addition, you agree that neither Customer, nor any of your employees or designated representatives, will use the Services in a manner that violates the laws, regulations, ordinances, or other such requirements of any jurisdiction.

In addition, Customer agrees that neither it, nor any of its employees or designated representatives, will: transmit any unsolicited commercial or bulk email, will not engage in any activity known or considered to be "spamming" and carry out any "denial of service" attacks on any other website or Internet service; infringe on any copyright, trademark, patent, trade secret, or other proprietary rights of any third party; collect, attempt to collect, publicize, or otherwise disclose personally identifiable information of any person or entity without their express consent (which may be through the person or entity's registration and/or subscription to Customer's services, in which case Customer must provide a privacy policy which discloses any and all uses of information that you collect) or as otherwise required by law; or, undertake any action which is harmful or potentially harmful to EMD or its infrastructure.

Customer is solely responsible for ensuring that its login information is utilized only by Customer and Customer's authorized users and agents. Customer's responsibility includes ensuring the secrecy and strength of user identifications and passwords. EMD shall have no liability resulting from the unauthorized use of Customer's login information. If login information is lost, stolen, or used by unauthorized parties or if Customer believes that any hosted applications or hosted data has been accessed by unauthorized parties, it is Customer's responsibility to notify EMD immediately to request the login information be reset or unauthorized access otherwise be prevented. EMD will use commercially reasonable efforts to implement such requests as soon as practicable after receipt of notice.

Licenses

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.