Cybersecurity Incident Response Procedure

Purpose

The purpose of this procedure is to establish a coordinated response to cybersecurity incidents that may affect the confidentiality, integrity, or availability of district information systems, student records, employee information, instructional technology, and school operations.

Scope

This procedure applies to all district employees, students, volunteers, contractors, and third-party vendors who access district technology resources.

Definition of a Cybersecurity Incident

A cybersecurity incident includes, but is not limited to:

- Ransomware attacks
- Malware or virus infections
- Unauthorized access to district systems
- Data breaches involving student or employee information
- Phishing attacks resulting in credential compromise
- Denial-of-service attacks
- Loss or theft of district-owned devices containing sensitive information
- Unauthorized disclosure of confidential information

Incident Command Structure

Incident Commander

- Superintendent or designee
- Provides overall leadership and decision-making authority.

Cybersecurity Response Coordinator

- Technology Director or Network Administrator
- Leads technical response efforts.

Public Information Officer

- Superintendent or Designee
- Coordinates all communications with staff, parents, media, and external agencies.

Legal and Compliance Advisor

- District administration and legal counsel
- Ensures compliance with state and federal reporting requirements.

School Administrators

- Coordinate school-level operations and continuity of learning.

Response Procedures

Phase 1: Identification

Staff Responsibilities

Any employee who discovers a suspected cybersecurity incident shall:

1. Immediately stop using the affected device if malicious activity is suspected.
2. Disconnect the device from the network if instructed by the Technology Department.
3. Report the incident immediately to the Technology Department.
4. Preserve any suspicious emails, messages, or screenshots.

Technology Department Responsibilities

1. Assess the scope and severity of the incident.
2. Determine affected systems and users.
3. Document:
    - Date and time discovered
    - Reporting party
    - Systems affected
    - Initial observations

Phase 2: Containment

Immediate Actions

The Technology Department shall:

For Malware or Ransomware

- Isolate infected devices from the network.
- Disable affected user accounts.
- Block malicious IP addresses and domains.
- Prevent lateral movement throughout the network.

For Account Compromise

- Disable affected accounts.
- Force password resets.
- Revoke active sessions and tokens.
- Enable additional monitoring.

For Data Breaches

- Restrict access to affected systems.
- Preserve evidence for investigation.
- Determine whether personally identifiable information (PII) was accessed.

Phase 3: Notification

Internal Notification

The Technology Director shall notify:

- Superintendent
- Appropriate school administrators
- Business Administrator (if financial systems are involved)
- Safety and Emergency Management Coordinator

External Notification

As required by law and district policy:

- Law enforcement
- Cybersecurity insurance provider
- Legal counsel
- State agencies
- Affected students, parents, or employees

Communication Guidelines

All public statements shall be approved by the Superintendent or designated Public Information Officer.

Employees shall not communicate incident details publicly or through social media.

Phase 4: Eradication and Recovery

Technology Department Actions

1. Remove malware and malicious files.
2. Patch vulnerabilities.
3. Restore systems from verified backups.
4. Verify system integrity before returning systems to production.
5. Increase monitoring of affected systems.

Recovery Priorities

Priority 1:

- Student Information System
- Emergency communication systems
- Internet connectivity
- Phone systems
- Financial and payroll systems

Priority 2:

- Staff email
- Security systems

Priority 3:

- Classroom instructional systems
- Auxiliary applications

Continuity of Operations

If critical systems are unavailable:

School Administrators Shall

- Implement manual attendance procedures.
- Use alternative communication methods.
- Utilize paper-based instructional materials as needed.
- Maintain continuity of educational services.

Technology Department Shall

- Establish temporary workarounds.
- Coordinate restoration efforts.
- Provide regular status updates.

Evidence Preservation

The Technology Department shall:

- Preserve system logs.
- Maintain forensic images when appropriate.
- Document all response actions.
- Record timelines and decisions.

No employee shall delete files or alter evidence related to a cybersecurity incident unless directed by the Technology Department.

Post-Incident Review

Within 30 days following recovery:

The Incident Response Team Shall

1. Conduct an after-action review.
2. Identify lessons learned.
3. Review effectiveness of response procedures.
4. Update cybersecurity controls.
5. Recommend policy or training improvements.

Report Components

- Incident summary
- Root cause analysis
- Impact assessment
- Actions taken
- Recovery timeline
- Recommendations

Training and Preparedness

The district shall:

- Provide annual cybersecurity awareness training for all employees.
- Conduct phishing awareness exercises.
- Review incident response procedures annually.
- Test backup restoration procedures at least annually.
- Include cybersecurity incidents in emergency management exercises when feasible.