

Risk Management Practices

1. Purpose

This document establishes the District's formal risk management practices for identifying, assessing, prioritizing, and mitigating risks to District data, information systems, technology infrastructure, instructional platforms, and operational processes. These practices support the protection of student, employee, financial, operational, and safety-related information in accordance with federal and state law, Board policy, and accepted cybersecurity and governance standards. The purpose of this document is to ensure that risk is reduced to an acceptable level while maintaining instructional continuity, operational efficiency, legal compliance, and public trust.

2. Scope

These risk management practices apply to all District-owned, leased, hosted, or managed:

- Wired and wireless data networks
- Internet connectivity and filtering systems
- Servers, virtualization platforms, storage, and backup systems
- Cloud services, SaaS applications, and instructional technology platforms
- Student information systems and learning management systems
- End-user devices, including desktops, laptops, Chromebooks, tablets, mobile devices, and classroom displays
- Security systems, surveillance systems, and access control platforms
- Third-party systems that store, process, or transmit District data
- Manual, paper-based, and operational procedures involving confidential information
- Data governance procedures, retention, access controls, and destruction workflows

This document applies to all employees, contractors, vendors, volunteers, and approved third parties with access to District systems or data.

3. Risk Assessment Requirements

A thorough risk analysis of District networks, systems, policies, procedures, and operational workflows shall be conducted:

- As needed based on identified concerns, incidents, or environmental changes
- Upon request of the Superintendent
- Prior to major system implementations or infrastructure changes
- Following any significant cybersecurity incident, data breach, service disruption, or natural disaster event
- As part of periodic governance reviews directed by the Superintendent or designee
- During review of new third-party applications, digital services, or data-sharing agreements

The Superintendent or designee shall ensure periodic risk assessments are administered to identify, quantify, document, and prioritize risks.

At minimum, the assessment process shall evaluate:

1. **Threat source** — internal, external, natural, accidental, or malicious
 2. **Likelihood** of occurrence
 3. **Operational and instructional impact**
 4. **Legal and regulatory exposure**
 5. **Data sensitivity and confidentiality level**
 6. **Existing controls and their effectiveness**
 7. **Residual risk after mitigation**
-

4. Risk Categories

District risk assessments shall include, but are not limited to, the following categories:

A. Cybersecurity and Technical Risks

- Unauthorized access or privilege escalation
- Malware, ransomware, phishing, and social engineering
- Weak passwords or lack of multifactor authentication
- Unpatched systems and unsupported software
- Network misconfiguration or segmentation failures
- Data exfiltration or unauthorized sharing
- Cloud platform misconfiguration
- Backup corruption or failed recovery procedures
- Identity and access management weaknesses
- Endpoint compromise or unmanaged devices

B. Operational Risks

- Inadequate procedures or inconsistent implementation
- Insufficient staff training or awareness
- Shadow IT and unapproved software usage
- Improper asset disposal or media sanitization
- Incomplete onboarding/offboarding processes
- Inadequate change management
- Lack of documentation or disaster recovery testing

C. Compliance and Legal Risks

- FERPA violations
- COPPA and student privacy noncompliance
- CIPA filtering failures
- Records retention violations
- Alabama state records and public education requirements
- Contractual and DPA noncompliance by vendors
- Improper disclosure of personnel or financial records

D. Physical and Environmental Risks

- Fire, severe weather, flooding, and tornado events
- Power loss and UPS/generator failure
- Unauthorized physical access to MDF/IDF/server rooms
- Theft or damage of mobile devices
- HVAC failure affecting network/server infrastructure
- Building access failures impacting security systems

E. Instructional Continuity Risks

- LMS or SIS outage during instruction or testing
 - Internet/WAN failure affecting digital learning
 - State testing platform disruptions
 - Loss of classroom instructional devices
 - Failure of classroom display or collaboration systems
-

5. Risk Rating and Prioritization

All identified risks shall be assigned a rating based on **likelihood, impact, and recoverability**.

Suggested Risk Levels

- **Critical** – Immediate threat to safety, student data, payroll, finance, state testing, or districtwide operations
- **High** – Significant disruption or likely legal/compliance exposure
- **Moderate** – Localized impact with manageable recovery path
- **Low** – Minimal operational impact or low likelihood

Critical and High risks shall require documented mitigation actions, assigned ownership, and target completion dates.

6. Risk Mitigation Requirements

The results of each assessment shall serve as the basis for a formal mitigation plan designed to reduce vulnerabilities and risk exposure to an acceptable level.

Mitigation measures may include:

- Administrative safeguards
 - Policy revisions
 - Procedure updates
 - staff training and awareness
 - role-based access reviews
- Technical safeguards
 - MFA enforcement
 - network segmentation
 - EDR/XDR protections
 - patching and vulnerability remediation
 - immutable backups and disaster recovery controls
 - logging, SIEM, and alerting
- Physical safeguards
 - controlled facility access
 - surveillance and door access controls
 - redundant power and environmental monitoring
- Contractual safeguards
 - DPAs
 - minimum security requirements
 - breach notification clauses
 - annual vendor review

Mitigation efforts shall prioritize reducing:

- Attack surface
 - Data exposure
 - Scope of access
 - Recovery time objectives
 - Single points of failure
 - Human process errors
-

7. Roles and Responsibilities

Superintendent

- Directs risk assessment activities as needed
- Reviews significant findings and unresolved high-risk items

- Authorizes districtwide mitigation priorities and resource allocation

Superintendent Designee / Director of Technology

- Administers periodic risk assessments
- Maintains the district risk register
- Coordinates remediation plans across departments
- Reports significant risks to District leadership
- Ensures annual review of critical systems and vendors

Department Leaders and Principals

- Participate in risk identification for operational and instructional systems
- Ensure local procedures align with District controls
- Report process weaknesses and recurring issues

Employees

- Follow approved policies and procedures
 - Immediately report suspicious activity, data incidents, or system misuse
 - Refrain from installing or using unapproved systems or applications
-

8. Documentation and Evidence

The District shall maintain documentation supporting all risk management activities, including:

- Risk assessments and supporting evidence
- Vulnerability scan summaries
- Security review findings
- Incident post-mortem reports
- Disaster recovery and backup test results
- Third-party security reviews
- Corrective action plans
- Exceptions and accepted residual risk approvals

Documentation shall be retained in accordance with District records retention schedules and applicable law.

9. Continuous Review and Improvement

Risk management is a continuous process. Findings from assessments, incidents, audits, technology reviews, insurance recommendations, and changes in law or threat landscape shall be used to strengthen District safeguards.

This document shall be reviewed:

- Annually
 - Following major technology or legal changes
 - After significant cybersecurity incidents
 - Upon Superintendent request
-

10. Acceptance of Residual Risk

When a risk cannot be fully mitigated due to financial, technical, operational, or instructional constraints, the Superintendent or designee may formally accept the residual risk when:

- The remaining exposure is documented
- Compensating controls are in place
- Legal compliance is maintained
- The acceptance decision is reviewed periodically

No residual risk may be accepted if it knowingly places protected student data, employee records, or safety systems at unreasonable risk.