Adopted: 03/21/16
Reviewed: 1/21/26
Revised: 9/19/2022, 5/18/2026

731R Information Security Governance and Cybersecurity Risk Management

I. PURPOSE

The purpose of this policy is to establish governance for the protection of Rockford Area Schools information systems, technology infrastructure, and data. Information technology systems and data are essential to district operations and must be protected from unauthorized access, disclosure, alteration, disruption, or destruction.

This policy establishes the framework for the district's Information Security Program and provides direction for protecting the confidentiality, integrity, and availability of district information resources.

The district's cybersecurity and information security program align with nationally recognized cybersecurity frameworks and guidance including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0)
- Cybersecurity and Infrastructure Security Agency (CISA) K–12 Cybersecurity Guidance
- CIS Critical Security Controls
- ISO/IEC 27002:2022 Information Security Controls

II. GENERAL STATEMENT OF POLICY

Rockford Area Schools shall maintain a comprehensive Information Security Program designed to protect district information resources, reduce cybersecurity risk, and ensure compliance with applicable laws and regulations.

The district will implement administrative, technical, and physical safeguards to protect district data and systems from unauthorized access, misuse, disruption, or loss.

Information security responsibilities extend to all district employees, students, contractors, volunteers, and third parties who access district systems or data.

The Superintendent shall establish and maintain administrative procedures, operational standards, and technical safeguards necessary to implement this policy.

III. SCOPE

This policy applies to all district information systems and information assets including:

- District-owned computers, devices, and equipment
- Network infrastructure and communications systems
- Cloud-based systems and hosted services
- Software and applications used to support district operations
- Data created, received, stored, or transmitted by the district

This policy also applies to third-party vendors and service providers that store, process, transmit, or access district data.

IV. INFORMATION SECURITY GOVERNANCE

The district shall maintain governance processes to oversee cybersecurity risk management and the protection of district information assets.

Information security governance responsibilities include:

- Oversight of cybersecurity risk management
- Implementation of district information security policies and procedures
- Compliance with applicable federal and state laws
- Cybersecurity incident response coordination
- Oversight of vendor and third-party data security
- Oversight of cybersecurity program maturity and performance metrics

The Superintendent shall designate a district Information Security Representative responsible for administration of the district's Information Security Program.

Cybersecurity Governance Committee

The district shall maintain a Cybersecurity Governance Committee consisting of representatives from Technology, Administration, Operations, and other relevant departments. The committee shall provide oversight of cybersecurity risk management, policy development, and incident response coordination.

V. ROLES AND RESPONSIBILITIES

1. School Board

The School Board provides governance oversight through adoption and periodic review of district information security policies.

2. Superintendent

The Superintendent is responsible for:

- Ensuring implementation of this policy
- Designating a district Information Security Representative
- Ensuring appropriate resources are available to support cybersecurity protections

3. Director of Technology

The Director of Technology is responsible for administration of the district's Information Security Program including:

- Network and infrastructure security
- Identity and access management
- Endpoint protection and monitoring
- Security monitoring and vulnerability management
- Backup and disaster recovery systems
- Coordination of cybersecurity incident response

The Director of Technology shall provide an annual report to the School Board summarizing:

- The district's cybersecurity risk posture
- Significant cybersecurity incidents
- Program maturity metrics and improvement efforts

4. Information Security Representative

The designated Information Security Representative shall support administration of the district's cybersecurity program and maintain professional knowledge and competency in cybersecurity practices through continuing professional education and relevant professional training.

5. District Administrators

District administrators are responsible for supporting implementation of district information security policies and ensuring staff compliance with data protection requirements.

6. Employees and Authorized Users

All employees and authorized users of district technology systems are responsible for:

- Protecting district data from unauthorized disclosure
- Following district information security and technology policies
- Reporting suspected cybersecurity incidents or vulnerabilities to the Technology Department or designated Information Security Representative

Failure to comply with district security policies may result in disciplinary action.

VI. INFORMATION SECURITY PROGRAM REQUIREMENTS

The district shall maintain an Information Security Program that includes the following components:

1. Cybersecurity Risk Management

The district shall conduct cybersecurity risk assessments at least annually and when significant changes to district technology systems occur.

The district shall maintain a cybersecurity risk register documenting identified risks, mitigation strategies, and responsible owners.

2. Access Control

The district will implement controls to ensure that access to district systems and data is restricted to authorized users based on job responsibilities. Security controls may include:

- Role-based access controls
- Least-privilege access
- Multi-factor authentication for administrative accounts, remote access, and access to sensitive systems

3. Endpoint and Network Security

The district will implement safeguards to protect network infrastructure and computing devices including endpoint protection technologies, network security controls, and vulnerability management.

4. Security Logging and Monitoring

The district shall maintain centralized security logging and monitoring capabilities designed to detect suspicious or malicious activity across district systems and networks.

5. Backup, Recovery, and Business Continuity

The district shall maintain secure backup systems, disaster recovery capabilities, and business continuity planning processes to ensure restoration of critical services following cybersecurity incidents or operational disruptions.

6. Security Awareness Training

District employees shall participate in periodic cybersecurity awareness training designed to reduce risks associated with phishing, social engineering, and other cyber threats.

VII. DATA CLASSIFICATION AND PROTECTION

The district shall maintain a formal data classification and handling framework consistent with the Minnesota Government Data Practices Act.

Data classification categories may include:

- Public Data
- Private Data
- Confidential Data
- Security Information

Appropriate safeguards shall be applied based on the classification and sensitivity of the data.

VIII. CYBERSECURITY INCIDENT RESPONSE

Rockford Area Schools shall maintain a documented Cybersecurity Incident Response Plan defining response role, escalation procedures, communication protocols, and recovery processes.

Incident response procedures shall address:

- Detection and reporting of cybersecurity incidents
- Incident containment and mitigation
- Notification to district leadership
- Compliance with state and federal breach notification requirements
- Coordination with law enforcement when appropriate
- Coordination with cyber insurance providers

All suspected cybersecurity incidents must be reported immediately to the Technology Department or designated Information Security Representative.

IX. VENDOR AND THIRD-PARTY SECURITY

Vendors and service providers that process, store, transmit, or access district data must comply with district security requirements and applicable laws. Vendors must notify the district of any security incident involving district data within a defined timeframe consistent with contractual obligations and applicable law.

Vendor agreements shall include provisions addressing:

- Data protection and privacy requirements
- Compliance with FERPA and applicable laws
- Security safeguards
- Breach notification obligations

The district shall conduct security evaluation of vendors that store, process, or access district data prior to contract approval and periodically thereafter.

X. EMERGING TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

The district shall evaluate cybersecurity, privacy, operational, and data protection risks associated with emerging technologies including artificial intelligence systems, connected devices, advanced analytics platforms, and new cloud-based services.

Use of artificial intelligence technologies that process, analyze, store, or generate district data must comply with district information security requirements, student data privacy protections, and applicable federal and state laws including the Family Educational Rights and Privacy Act (FERPA) and the Minnesota Government Data Practices Act.

Artificial intelligence technologies that access district systems or data may be subject to security and privacy review prior to implementation to ensure appropriate safeguards are in place.

The district may establish administrative procedures governing the evaluation, procurement, and use of artificial intelligence technologies to ensure responsible use, protection of student and staff data, and alignment with district instructional and operational goals.

XI. POLICY REVIEW

This policy shall be reviewed annually to ensure alignment with evolving cybersecurity threats, legal requirements, emerging technologies, and industry best practices.

This policy establishes governance and oversight expectations for the district's information security program and is not intended to serve as a technical or operational manual. Specific security procedures, technical controls, and operational practices may be modified by the district as necessary to address evolving cybersecurity risks, technology changes, and operational requirements.

Legal References

Minn. Stat. Ch. 13 – Minnesota Government Data Practices Act
Minn. Stat. § 13.055 – Security Breach Notification
Minn. Stat. § 13.37 – Security Information
Minn. Stat. § 16E.36 – State Cybersecurity Program
Minn. Stat. § 125B.15 – Internet Access for Students

Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. §1232g
Children's Online Privacy Protection Act (COPPA) – 15 U.S.C. §6501 et seq.
Children's Internet Protection Act (CIPA) – 47 U.S.C. §254

Cross References

Policy 406 – Public and Private Personnel Data
Policy 515 – Protection and Privacy of Pupil Records
Policy 524 – Internet Acceptable Use and Safety
Policy 722 – Public Data Requests
Policy 806 – Crisis Management