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

¶

731R INFORMATION SECURITY POLICY ¶

¶

I. **PURPOSE** ¶

¶

The purpose of this policy is to authorize and direct the Superintendent to establish, implement, educate, and maintain a data governance plan comprised of a series of information technology security protocols and procedures.¶

¶

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions; vital curricular functions; compromise data; and result in legal and regulatory non-compliance.¶

¶

This policy benefits all stakeholders of Rockford Area Schools by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.¶

¶

II. Scope¶

¶

This policy encompasses all systems, automated and manual, for which Rockford Area Schools has administrative responsibility, including systems managed or hosted by third parties on behalf of the entity. It addresses all information, regardless of the form or format, which is created or used in support of School District activities.¶

¶

Information security measures apply to all Rockford Area Schools agents and employees and all district operations. Any unauthorized access, use, transfer, or distribution of district information by any employee, affiliated or non-affiliated vendor, student, or any other individual, may result in appropriate disciplinary action, which may include a recommendation for termination and other legal action.¶

¶

III. General Statement of Policy¶

¶

This policy acts as an umbrella document to all other security policies and ¶
associated standards. This policy defines the responsibility to:¶

¶

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;¶
- manage the risk of security exposure or compromise;¶
- assure a secure and stable information technology environment;¶

- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;¶
- monitor systems for anomalies that might indicate compromise; and¶
- promote and increase the awareness of information security. ¶

¶

IV. Functional Responsibility and Requirement¶

The District Administrative Team is responsible for:¶

1. evaluating data security risks on behalf of the entity;¶
2. identifying information security responsibilities and goals and integrating them into their relevant program or department processes;¶
3. supporting the consistent implementation of information security policies, protocols and standards;¶
4. supporting security through clear direction and demonstrated commitment of appropriate resources;¶
5. promoting awareness of information security best practices through the regular dissemination of materials provided by the Superintendent or designated information security representative;¶
6. implementing the process for determining information classification and categorization, based on legal and regulatory requirements to determine the appropriate levels of protection for that information;¶
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;¶
8. participating in the response to security incidents;¶
9. complying with notification requirements in the event of a breach of private information, including the requirements in Minnesota Statutes § 13.055;¶
10. adhering to specific legal and regulatory requirements related to information security;¶
11. communicating legal and regulatory requirements to the Superintendent or designated information security representative; and¶
12. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.¶

The Superintendent or designated information security representative is responsible for:¶

1. maintaining familiarity with School District functions and requirements;¶
2. maintaining an adequate level of current knowledge and proficiency in information security through annual continuing professional education directly related to information security;¶
3. assessing compliance with information security policies and legal and regulatory information security requirements;¶
4. evaluating and understanding information security risks and how to appropriately manage those risks;¶
5. representing and assuring security architecture considerations are addressed; ¶
6. determine appropriate access permissions in order for staff to complete their duties.¶
7. advising on security issues related to procurement of products and services;¶
8. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;¶

9. disseminating threat information to appropriate parties;¶
10. participating in the response to potential security incidents; ¶
11. ensuring new employees are provided with instruction and/or documented procedures that relate to their job descriptions;¶
12. participating in the development of district wide protocols and procedures that considers the School District's needs; and¶
13. promoting information security awareness.¶

The Director of Technology and Information Services is responsible for:¶

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s);¶
2. providing resources needed to maintain a level of information security control consistent with this policy;¶
3. identifying and implementing all processes, policies, protocols and controls relative to security requirements defined by federal, state, various regulatory agencies, and this policy; ¶
4. implementing the proper controls for information owned based on the data classification designations;¶
5. providing training to appropriate staff or other stakeholders on secure operations (e.g., user access, social media, data privacy);¶
6. report to the Rockford Area Schools Board of Directors annually and submit interim reports at the request of the Superintendent, on the current status of the school district technology protocols and procedures¶
7. fostering the participation of information security with staff and other stakeholders in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and¶
8. implementing business continuity and disaster recovery plans.¶

All employees and other individuals performing services on behalf of the School District that involve the access, use, or creation of government data are responsible for:¶

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;¶
2. protecting information and resources from unauthorized use or disclosure;¶
3. informing the Superintendent and Information Security designee(s) if there are any problems with an established protocol or procedure or if they are aware of concerns about compliance with a defined protocol or procedure;¶
4. protecting private, confidential, and non-public data from unauthorized use or disclosure;¶
5. Any individual granted access to private data is responsible for maintaining the privacy of that data and complying with applicable data privacy rules and policies. Access will be used only in accordance with the authority delegated to the individual to conduct district operations.¶
6. It is the express responsibility of authorized users to safeguard the information they are entrusted with, ensuring compliance with all aspects of this policy and additional related district policies and/or procedures.¶
7. These security measures apply to district information regardless of location. Users who transfer or transport district information "off-campus" for any reason must ensure that they are able to

comply with all information security measures prior to transporting or transferring the information.¶

8. abiding by Internet Acceptable Use and Safety Policy – Policy 524; and¶
9. reporting suspected information security incidents or weaknesses to the Director of Technology and Superintendent or the designated information security representative.¶

V. Policy Review¶

¶

This policy will be reviewed on an annual basis.¶

¶

Legal References: ¶

Minn. Stat. § 121A.75 (Receipt of Records; Sharing)¶

Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)¶

Minn. Stat. § 13.05 subd. 5 (Data Protection)¶

Minn. Stat. § 13.055 subd. 6 (Security Assessments) ¶

Minn. Stat. § 13.393 (Attorneys)¶

15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act) ¶

17 U.S.C. § 101 et seq. (Copyrights) ¶

20 U.S.C. § 1232G (Family Educational Rights and Privacy Act) ¶

34 C.F.R. § 300.610-300.627 (Confidentiality of Information)¶

47 U.S.C. § 254 (Children's Internet Protection Act of 2000(CIPA)) ¶

47 C.F.R. § 54.520 (FCC rules implementing CIPA) ¶

Public Law No. 113-283 (12/18/2014)¶

Strengthening American Cybersecurity Act of 2022 (March 2022) S.360¶

Minn. Stat. § 121A.031 (School Student Bullying Policy) ¶

Minn. Stat. § 125B.15 (Internet Access for Students) ¶

Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act) ¶

¶

¶

Cross References:¶

MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District ¶ Employees) ¶

MSBA/MASA Model Policy 406 (Public and Private Personnel Data) MSBA/MASA Model Policy ¶ 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and ¶ Employees) ¶

MSBA/MASA Model Policy 506 (Student Discipline) ¶

MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records) MSBA/MASA Model ¶ Policy 519 (Interviews of Students by Outside Agencies) MSBA/MASA Model Policy 521 (Student ¶ Disability Nondiscrimination) MSBA/MASA Model Policy 522 (Title IX Sex Nondiscrimination ¶ Grievance Procedures and Process) ¶

MSBA/MASA Model Policy 603 (Curriculum Development) ¶

MSBA/MASA Model Policy 604 (Instructional Curriculum) ¶

MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials) ¶

MSBA/MASA Model Policy 722 (Public Data Requests) ¶

MSBA/MASA Model Policy 806 (Crisis Management Policy) ¶

MSBA, School Law Bulletin "I" (School Records – Privacy – Access to Data)¶

NIST Cybersecurity Framework – Policy Template Guide – cisecurity.org/ms-isac/