Adopted: 03/21/16
Reviewed: _____
Revised: 9/19/2022

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/