Minneota Public School District
District Procedures

Adopted: February 2023

Updated: October 2024

DISTRICT PROCEDURES: SECURITY AWARENESS AND TRAINING PROCEDURES

1. PURPOSE

1.1 Access to Information Technology (IT) in Minneota Public Schools is for educational and business-financial-human resources purposes. The use of the district's electronic technologies is a valued resource for our students, families, staff, and community and needs to be safe, appropriate, and aligned with the mission and vision of the district. The main purposes of these procedures are to:

1.1.1 ensure that the appropriate level of information security awareness training is provided to all Information Technology (IT) users,

1.1.2 provide appropriate cybersecurity in and for the district, and

1.1.3 protect Information Technology (IT) from unauthorized access, modification, destruction, or disclosure.

2. DISTRICT PROCEDURES

2.1 These procedures are applicable to all departments and users of IT resources and assets.

3. SECURITY AWARENESS TRAINING

3.1 Minneota Public Schools shall:

3.1.1 Schedule security awareness training as part of initial training for new users.

3.1.2 Schedule security awareness training when required by information system changes and then monthly thereafter.

3.1.3 IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

3.1.3.1 Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

3.1.3.2 Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

4. SECURITY AWARENESS | INSIDER THREAT

4.1 The IT Department shall include security awareness training on recognizing and reporting potential indicators of insider threat.

5. ROLE-BASED SECURITY TRAINING

5.1 The IT Department shall:

5.1.1 Provide role-based security training to personnel with assigned security roles and responsibilities.

5.1.2 Before authorizing access to the information system or performing assigned duties.

5.1.3 When required by information system changes and yearly thereafter.

5.2 Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

6. PHYSICAL SECURITY CONTROLS

6.1 The IT Department shall:

6.1.1 Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

6.1.2 Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

7. PRACTICAL EXERCISES

7.1 The IT Department shall provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives.

7.1.1 These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

8. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

8.1 The IT Department shall provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

9. SECURITY TRAINING RECORDS

9.1 Minneota Public Schools shall:

9.1.1 Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

9.1.2 Retain individual training records for the time that the employee is employed at the district.

10. COMPLIANCE

10.1 Employees who violate these procedures may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual

agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

11. PROCEDURES - EXCEPTIONS

11.1 Requests for exceptions to these procedures shall be reviewed by the Technology Director and Superintendent. Departments requesting exceptions shall provide such requests to these staff members. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein. The Technology Director and Superintendent shall review such requests and confer with the requesting department.

12. RESPONSIBILITIES

12.1 The Technology Director and Superintendent are responsible for updating and maintaining these procedures, along with compliance with the procedures.

13. REFERENCES AND RESOURCES

13.1 National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301