Minneota Public School District
District Procedures

Adopted: September 2025

DISTRICT PROCEDURES: ACCESS CONTROL

1. **PURPOSE**

   This document outlines the procedures for securely logging onto the district's network and systems to ensure the protection of sensitive information and prevent unauthorized access.

2. **SCOPE**

   This procedure applies to all employees, contractors, and third-party vendors who require access to the company's network and systems.

3. **PROCEDURE:**

   User Account Creation:

   3.1 User accounts will only be created for individuals authorized by their respective department heads or supervisors.

   3.2 Each user account will be associated with a unique username and a strong, complex password.

   3.3 Passwords must adhere to the districts password policy, which includes requirements for length, complexity, and regular expiration.

   Access Control:

   3.4 Users will only be granted access to the systems and resources necessary for the performance of their job duties.

   3.5 Access permissions will be reviewed and updated at least bi-annually to reflect changes in job responsibilities or employment status.

   Authentication:

   3.6 Users may be required to authenticate themselves using their unique username and password.

   3.7 Multi-factor authentication (MFA) may be implemented to add an extra layer of security. This may include the use of hardware tokens, mobile authentication apps, or biometric authentication where applicable.

   Remote Access:

   3.8 Remote access to the districts network and systems will be granted only through secure channels such as virtual private networks (VPNs) or remote desktop gateways.

   3.9 Remote users must adhere to the same authentication and access control procedures as on-site users.

Session Management:

3.10 Users are required to log off from their accounts or lock their screens when leaving their workstations unattended.

3.11 Inactive sessions will be automatically logged off after a predefined period of inactivity to prevent unauthorized access.

Password Management:

3.12 Passwords must not be shared with anyone, including colleagues or IT support staff.

3.13 Users must change their passwords periodically as per the district's password policy.

3.14 Passwords should be stored securely using industry–standard encryption techniques.

Monitoring and Logging:

3.15 User log-on and access activities will be monitored and logged for auditing and security analysis purposes.

3.16 Any suspicious or unauthorized log-on attempts will be investigated and reported to the appropriate authorities.

4. RESPONSIBILITIES

IT Department:

4.1 Create and manage user accounts.

4.2 Enforce password policies and access controls.

4.3 Monitor and analyze log-on activates.

Employees:

4.4 Adhere to the procedures outlined in the document.

4.5 **Immediately** report any suspicious or unauthorized log-in attempts to the IT department.

4.6 Protect their passwords and authentication credentials.

5. COMPLIANCE

Employees who violate this procedure 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.

6. PROCEDURE EXCEPTIONS

Requests for exceptions to this procedure shall be reviewed by the Technology Director. Departments requesting exceptions shall provide such requests to the Technology Director. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact 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 shall review such requests and confer with the requesting department.

7. RESPONSIBLE DEPARTMENT

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