

# Mounds View Public Schools Ends and Goals Regulation

## **EG-0108      Technology Security**

Mounds View Public Schools depends upon its computer based information systems and the availability of its data and communication systems to support its academic vision and administration. The following regulation supports Policy EG-0108 and will constitute the District's technology security protocol.

### **Definitions**

**SA**      System Administrator - person responsible for the configuration or management of the technology resource

**User**     Person who receives or uses technology resources

**VPN**     Virtual Private Network - used to gain remote access to Mounds View's internal network

### **1.0 Desktop and Laptop Computers**

In order to protect the integrity of the District's electronic information systems, the following steps must be adhered to by both system administrators (SA) and end users (Users).

1. All district-owned desktop and laptop computers must use district approved security software that protects against configuration drift, accidental system misconfiguration, malicious software activity, and incidental system degradation. (Users)
2. Laptop and desktop computers will be secured through the use of effective passwords as identified in section 7.0 – Passwords. (SA, Users)
3. The computers BIOS will be password protected to prevent unauthorized access to the computer. (SA)
4. All district owned computers need to be running district approved anti-virus software and should be patched with the latest definitions. (SA)
5. Unattended computers must be logged out to prevent unauthorized users from compromising data. (SA, Users)
6. Data needs to be stored on each users personal home folder (P: drive) or in an appropriate networked shared resource (S: drive). Due to the nature of the District's security software, it becomes essential that data is stored in the proper location for it to be accessible and to ensure that your data is backed up. For more information regarding backups, see section 3.0 Backup and Restoration. (SA, Users)
7. All computers, especially laptops, must be physically secured. Make sure that unattended classrooms are locked and unused laptops are returned to a locked laptop mobile cart. Mobile carts, when not in use, should be stored in a secure location and keys to the carts should be stored in a designated area that is inaccessible to unauthorized users. (SA, Users)
8. Confidential and sensitive information must be safeguarded. Appropriate measures (e.g., encrypting electronic information, physically secure physical media, using caution when printing confidential information) must be taken to prevent unauthorized disclosure. (SA, Users)
9. Staff members who have been issued a district owned laptop are required to review and sign the EG-0108-F Laptop Care Agreement. (Users)
10. All computers will be pre-configured by district technology staff with separate accounts for system administrator, staff and student use. (SA)

# Mounds View Public Schools Ends and Goals Regulation

## EG-0108 Technology Security - continued

### 2.0 VPN

Approved Mounds View employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software and paying associated fees.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Mounds Views internal networks.
2. VPN use is to be controlled using a one-time password authentication.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Mounds View Public Schools Infratech network operational group.
6. All computers connected to Mounds Views internal networks via VPN or any other technology must use the most up-to-date, district approved anti-virus software (this includes personal computers).
7. VPN users will be automatically disconnected from Mounds View Public School's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. Users of computers that are not district-owned equipment must configure the equipment to comply with Mounds View's VPN and any other relevant policies.
9. Only Mounds View Infratech-approved VPN clients may be used.
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Mounds View's network and as such are subject to the same rules and regulations that apply to district-owned equipment, i.e., their machines must be configured to comply with all of the district's IT security policies and regulations.
11. Users can initiate a request for VPN access by calling the Mounds View Helpdesk @ x5000. Requests will be reviewed by the Infratech/Security group. Before being granted VPN access, users will be required to complete Form EG-0108-A Mounds View VPN Access Agreement.

### 3.0 Backup and Restoration

Mounds View Public School's requires that computer systems maintained by the District's technology department are backed up periodically and that the backup media is stored in a secure off-site location. The system's backups will consist of full and incremental backups on a regular schedule as defined by the District's technology department. The standard procedure for systems backup is as follows:

1. Full systems backup will be performed weekly. Weekly backups will be saved for 2 months.
2. Incremental backups will be performed daily.
3. All backups will be stored in a secure off-site location.
4. Periodic tests of the backups will be performed to ensure that data can be successfully restored.

All media that has reached its data retention schedule will be reused, recycled or destroyed. Backup media that is not reusable will be destroyed in an approved manner as defined in section 5.0 Technology Asset Management.

# Mounds View Public Schools Ends and Goals Regulation

## EG-0108 Technology Security - continued

The District's technology department does not backup data located on individual workstations. It is the responsibility of the user to make sure their data is copied to their network home folder (P: drive) or in an appropriate network shared resource (S: drive).

### 4.0 Wireless Communication

Access to Mounds View's data networks via unsecured wireless communication mechanisms is strictly prohibited. Only wireless systems that meet the criteria of this regulation or have been granted an exclusive waiver by Mounds View's technology department are approved for connectivity to the Mounds View data networks

#### Access Points and Associated Wireless Hardware

All wireless devices connected to the Districts data network must be approved and configured by the Mounds View Public School's technology department. These devices are subject to periodic penetration tests and audits.

#### Obtaining Wireless Hardware

All wireless LAN access must use district-approved vendor products and security configurations. Requests for hardware should be initiated by submitting Form EG-0108-B Hardware Request.

#### Encryption and Authentication

All implementations must support a hardware address that can be registered and tracked. i.e., a MAC address. All implementations must also support and employ strong encryption using WPA2 or greater security mechanisms.

#### Setting the SSID

The SSID will be configured so that it does not contain any identifying information about the organization, such as division title, employee name or product identifier.

### 5.0 Technology Asset Management

The District's technology department is responsible for the management of IT assets and lifecycle processes, including standards, acquisition, management, surplus and long-range planning. The responsibility lies with the technology department to ensure that IT assets are acquired, managed and disposed of in compliance with all federal, state and local laws and regulations. Consistency in technology allows the development of efficient and cost-effective methods for supporting and managing IT assets and in planning for upgrades, migrations, staff training and future installations.

1. All purchases must comply with State laws, Federal laws and guidelines, and Technology Minimum Standards.
2. Acquisition of hardware and/or software will follow a central purchasing method. Purchases, contracts, maintenance agreements and renewals will be processed through the District's technology department.
3. A technology minimum standards document will be established for Mounds View Public Schools. It will be defined and managed by the District's Director of Technology.

# Mounds View Public Schools Ends and Goals Regulation

## EG-0108 Technology Security - continued

4. Approvals for acquisition will be based on availability of funds, conformance to technology minimum standards and match for business need.
5. Requests for technology hardware or software can be initiated by submitting its corresponding request Form EG-0108-B Hardware Request and/or Form EG-0108-C Software Request.
6. Any technology assets acquired for or on behalf of the District will be deemed property of Mounds View Public Schools.
7. Technology assets must be disposed of in a manner that complies with all state, federal and local laws and regulations. IT assets that are no longer in use are required to be recycled through the District's technology department. Requests for Recycling services can be initiated using Form EG-0108-D IT Asset Disposal.

## 6.0 Passwords

Passwords are an important component of information and network security. The use of a user id and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the District can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met. The purpose of this regulation is to provide the guidelines necessary for the entire Mounds View Public School's data network to create appropriate passwords and to use them and protect them in an appropriate manner.

1. Password construction, lifecycle and re-use parameters will be variable according to the classification of the system or data that they are intended to protect.
2. Passwords cannot be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.
3. Users will be notified one week in advance of password expiration. At that point, users will be prompted to select a new password. Failure to change your password during this "grace login" will result in the user being locked out of the workstation requiring assistance from the technology helpdesk to reset the user's password.
4. All passwords must conform to the guidelines outlined below.

# Mounds View Public Schools Ends and Goals Regulation

## EG-0108 Technology Security - continued

### 6.1 Password Construction

Require unique passwords = True

Minimum number of characters in password = 8

Max number of times a specific character can be repeated sequentially = 4

Disallow numeric as first character = yes

Minimum number of numerals = 1

Minimum number of lowercase characters required = 1

Minimum number of upper case characters required = 1

Disallow special character as first character = yes

Minimum number of special characters = 1

### 6.2 Password Lifecycle

Users will be required to change their passwords a minimum of two times per school year. The technology helpdesk will send out a notification of upcoming password changes a minimum of one week prior to the password change date. On the day that passwords are set to expire, users will be prompted with a message asking them to change their password. If the password is not reset during this “grace login” period, the user will be locked out of their workstation and any subsequent login attempts will be unsuccessful.

### 6.3 Password Protection Guidelines

1. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell or hint at their password to another person, including administrators, superiors, other co-workers, friends and family members.
2. Under no circumstances will any member of the organization request a password without the request coming from a representative of the IT department. Should a request be made that does not come from a representative of the IT department, immediately inform both the IT department and your direct supervisor.
3. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled location if in hardcopy form or in an encrypted file if in electronic form.
4. Do not use the “Remember Password” feature of applications.

# Mounds View Public Schools Ends and Goals Regulation

## EG-0108 Technology Security - continued

5. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access district accounts.
6. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the technology helpdesk and the password changed immediately.
7. The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

## 7.0 Personal Electronic Devices

### Personal Laptops and Network Hardware

1. Connecting personal computers and network equipment (i.e. laptop or desktop computers, wireless access points, network switches or hubs) to the Mounds View system is strictly prohibited without an exclusive waiver (Form EG-0108-E Personal Computer Agreement) from the Districts Technology Department.

### Other Personal Equipment

Personal devices such as PDA's, traditional and smart cell phones are frequently involved in data security breaches, such as when the device falls into the hands of an unauthorized user through loss or theft. Many of these devices may be configured to access district information that is protected by law (restricted), and that is not approved for viewing by unauthorized persons (sensitive). Employees that use these types of devices to access the districts systems must protect the device by activating password protection along with the use of a strong password.

## 8.0 Incident Handling

Any effort to circumvent the security systems and procedures designed to prevent unauthorized access may result in suspension of access and appropriate disciplinary actions pursuant to EG-5104 Use of Technology - Employees and EG-2104 Use of Technology - Students. In addition, the technology department reserves the right to restrict the use of computers and network systems when it is necessary to do so to protect the integrity of the District's technology resources.

June 2, 2009