Board Security Policy Proposal

Information Security Policy

Purpose of this policy

- Define information assets as they pertain to this policy
- Describe how information assets will be protected
    - Responsibilities of users to protect information assets
    - Responsibilities of system administrators to protect information assets

Rationale

The value of the data, software, and hardware owned by the district has increased substantially since the technology program was first implemented. The time and financial resources required to recreate the knowledge currently on district computers, servers, and other technology assets are so large that steps need to be taken to protect and preserve that knowledge to avoid undue burden to the district.

It is the responsibility of every user to maintain the mindset of security while using district information assets.

Definition of Information Assets

Information assets include computer and peripheral equipment, communications equipment, computing and communications premises, power, environmental control and communications utilities, data storage media, system computer programs and documentation, application computer programs and documentation, and information (data) in any format stored on district owned equipment, servers, workstations or any other storage format.

Protecting Information Assets

User Responsibilities

- Users of the District 106 information network must treat information assets in a way that is consistent with the security of students, faculty, and the community.
- Users of the District 106 information network must treat information assets in a way that is consistent with the district's best financial and professional interests in mind. Intentional damage or destruction of information assets is unacceptable.
- Users may only store data on the information network in such locations and using such procedures as prescribed by District 106.
- The Board of Education of School District 106 or its designee may, at any time, examine, copy, move, or delete any information created, stored or

transmitted on the computing resources of District 106 without notice. Users should not maintain any expectation of privacy with regards to the district.
- Users of the District 106 information network will be issued a network account and/or an E-mail account.
    - Accessing another user's account or allowing another user to access your account on any district technology asset is strictly prohibited unless approval by the Director of Technology has been granted in advance.
    - Sharing your account password(s) with anyone except the Director of Technology or his assistants is strictly prohibited.
    - Account passwords must be rotated on such a schedule and in such a manner as prescribed in the District 106 Information Technology Procedures Manual.
    - Users of the District 106 information network should only remain logged into the system while they are actively using network resources.
- Users may not install ANY software to district owned information assets without prior written approval from the Director of Technology.
- No unauthorized computers, laptops, PDA's, storage media, nor any other device for the storage, transmission, reception, or processing of electronic information may be used on the district information network or in combination with district information assets without prior authorization from the Director of Technology.
- No encryption devices or software may be used on the district information network or in combination with district information assets without prior written authorization from the Director of Technology.
- Users must notify the Director of Technology immediately if they gain knowledge of breaches of security as defined by this policy.
- All staff and students agree to abide by this and all other district technology policies and procedures when they submit a signed acceptable use policy.

District Responsibilities

- The primary agent for implementing district responsibilities under this policy will be the Director of Technology and his assignees.
- The Director of Technology, as the head of the technology department at District 106, will be responsible for maintaining, updating, and reporting changes to the following documents which will detail the working application of this policy:
    - Acceptable Use Policy
    - District 106 Information Technology Procedures Manual
- The district is responsible for the integrity of all district owned information assets.

- The district will take appropriate steps to minimize the vulnerability of information assets to unauthorized users.
    - The district will install and maintain a firewall between the Internet and the private district network.
    - The district will employ an Internet filtering solution and maintain it in a way that is consistent with federal and state law, curricular goals, and acceptable use policies of the district.
    - The district may employ measures to minimize the impact of viruses, trojans, and/or worms on district information assets.
- The district will perform regularly scheduled backups of all network servers and other information assets as may become necessary.
    - A reasonable and functional backup retention policy will be created within the context of the District 106 Information Technology Procedures Manual
    - The district will maintain a secure offsite backup facility for storage of monthly backup media.
- The district may monitor the activities of users of District 106 information assets visually, via tracking software, logs, or remote access at any time.
    - The district may create and retain usage, access, and error logs on any and all activity that occurs on district information assets.
    - Monitoring shall be conducted to prevent access to inappropriate material, to prevent unauthorized alteration of computers, servers, or network equipment, or to insure the safety and security of students when using information assets.
- The district may employ desktop security software as necessary.
- The district will restrict physical access to all network infrastructure elements to ensure data integrity will not be compromised at the source.
- The district will maintain appropriate security measures on the District 106 website.
    - All grade level and/or subject oriented material posted to the District 106 web site will be approved by a building principal and the Director of Technology.
    - The Superintendent and the Director of Technology will approve all other posted information.
- The Director of Technology shall document all detected breaches of this security policy. The superintendent shall receive reports of breeches as soon as possible after each breach has occurred and been contained.

School District 106 is not responsible for any information that may be lost, damaged, or unavailable when using district information assets, or for any information that is retrieved via these systems. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to any technology system. Attempts to circumvent this policy or any part of it will be treated as if the attempted breach were successful.