SUBJECT: INFORMATION SECURITY

The purpose of this policy is to define a set of security requirements that the District will implement in order to safeguard vital district information. This policy shall serve as best practices for the District and all third parties conducting business within and/or for the District.

The primary objectives of this Information Security Policy are to:

- Effectively manage the risk of security exposure or compromise within the District.
- Communicate the responsibilities for the protection of District information.
- Preserve administration's options in the event of an information asset misuse, loss or unauthorized disclosure.
- Promote and increase the awareness of information security in the District.

This policy is applicable to the District, staff and all others, which have access to or manage District information. The District Information Security Policy encompasses all computer systems for which the District has administrative responsibility. It addresses all information regardless of the form or format, which is created or used in support of educational/business activities of the District. This policy must be communicated to all faculty, staff and all others who have access to or manage District information.

This Information Security Policy is a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the District's objectives. Compliance with this policy is mandatory. This Information Security Policy sets the direction, gives broad guidance and defines requirements for information security-related processes and actions throughout the District. This policy documents the security practices already in place within the District.

Information Policy

Information is among the District's most valuable assets, and the District relies upon that information to support its daily activities. The quality and availability of that information is key to the District's ability to carry out its mission. Therefore, the security of the District's information, and of the technologies and systems that support it, is the responsibility of everyone concerned. Each authorized user of the District's information has an obligation to preserve and protect District information in a consistent and reliable manner. Security controls provide the necessary physical, logical and procedural safeguards to accomplish those goals.

Information security management enables information to be shared while ensuring protection of that information and its associated computer assets including the network over which the information travels. District designated staff are responsible for ensuring that appropriate physical,

SUBJECT: INFORMATION SECURITY

logical and procedural controls are in place on these assets to preserve the security properties of confidentiality, integrity, availability and privacy of District information.

Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security.

- Access to District computers, computer systems and networks must be provided through the use of individually assigned unique user-IDs.
- Individuals who use District computers must only access information assets to which they are authorized.
- Associated with each user-ID is an authentication token, such as a password, which must be used to authenticate the person accessing the data, system, or network. Information used to authenticate the identity of a person or process must be treated as personal and must not be disclosed.
- Each individual is responsible to reasonably protect against unauthorized activities performed under their user-ID.
- For the user's protection, and for the protection of District resources, user-IDs and passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared.

Confidentiality/Integrity/Availability

All District information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity.

Appropriate processes will be defined in the District recovery plan and implemented to ensure the reasonable and timely recovery of all District information, applications, systems and security regardless of computing platform, should that information become corrupted, destroyed or unavailable for a defined period.

Physical Equipment Policy

Computer equipment must be physically protected from security threats and environmental hazards. Protection of computer equipment is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure. This protection will include but is not limited to data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

SUBJECT: INFORMATION SECURITY

Secure Disposal or Re-use of Storage Media and Equipment

There is risk of disclosure of District information through careless disposal or re-use of equipment. Formal processes must be established to minimize this risk. Storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store information) or paper containing District information must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive District information.

Clear Screen

To prevent unauthorized access to information, automated techniques and controls will be implemented to require authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.

Internet and Electronic Mail Acceptable Use

When District employees connect to the Internet using any District Internet address designation or send electronic mail using the District designation, it should be for purposes authorized by the District administration. The following is not an all-inclusive list, and provides only examples of behavior that could result in security breaches. Specifically, the Internet and electronic mail will not be used:

- To represent yourself as someone else (i.e., "spoofing");
- for spamming;
- for unauthorized attempts to break into any computing system whether district's or another organization's (i.e., cracking or hacking);
- for theft or unauthorized copying of electronic files;
- for posting District information without authorization from District's administration;
- for any activity that creates a denial of service, such as "chain letters"; for "sniffing" (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

SUBJECT: INFORMATION SECURITY

The District email system is to be used in the interest of the District, to support its educational, administrative and business goals. Employees will not use email for illegal, disruptive, unethical activities or for personal gain.

The Employee Computer Services & Internet Use Regulations and Procedures sets forth the District's regulations and procedures for the proper use of the District's computer equipment, network, Internet and district email from the District's computer terminals either in the District or remotely.

Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the District and outside of the District. Users of the District email system are a visible representative of the District and must use the systems in a legal, professional and responsible manner.

Portable Devices

All portable computing resources and information media must be secured to prevent compromise of confidentiality or integrity. No computer device may store or transmit District information without suitable protective measures that are approved by the District.

When using mobile computing equipment such as notebooks, PDAs, laptops, smartphones, cell phones and other mobile or wireless devices, special care must be taken to ensure that information is not compromised. Approval is contingent on satisfaction of the requirements for physical protection, access controls, cryptographic techniques, back-ups, virus protection and the rules associated with connecting mobile equipment to networks and guidance on the use of these facilities in public places.

- Care must be taken when using mobile computing equipment in public places, meeting rooms and other unprotected areas outside of the District premises. Protection must be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities.
- It is important that when such equipment is used in public places, care must be taken to avoid the risk of unauthorized persons viewing information on-screen.
- Procedures against the use of malicious software shall be developed and implemented and be kept up to date. Protocol will be established that will enable the quick and easy back up of information. These backups must be given adequate protection against theft or loss of information.
- Equipment containing District information must be attended at all times or physically secured.

SUBJECT: INFORMATION SECURITY

User Registration and Management

A user management process shall be established and documented by the District to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to the District applications and information and that these users only have access to the resources required for authorized purposes.

The user management process must include the following sub-processes as appropriate:

- Enrolling new users;
- removing user-IDs;
- granting "privileged accounts" to a user;
- removing "privileged accounts" from a user;
- periodic reviewing "privileged accounts" of users;
- periodic reviewing of users enrolled to any system; and
- assigning a new authentication token (e.g. password reset processing).

User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards must be developed and implemented to ensure all authorized individuals accessing District resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible. These password best practices include, but are not limited to:

- use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
- keep passwords confidential ~ do not share individual;
- change passwords at intervals;
- change temporary passwords at the first logon;
- passwords must contain a minimum of eight (8) mixed alphabetic, numeric, special, and upper/lower case characters.

Electronic Permissions

User's rights on the various network servers will be set according to the needs of the individual user. All users will have rights to their user directory. Any rights beyond that will need to be authorized by the Director of Technology under the advisement and oversight of the Superintendent of Schools.

SUBJECT: INFORMATION SECURITY

Anti-Virus/Anti-Spam

All computers in the District network must have Anti-virus programs installed and activated. Removal or de-activation of such programs will be considered a violation of the District policy. It is also a violation of this policy to knowingly introduce any harmful software with the intent of doing harm to the District's computer systems.

Networking Equipment

It is against and in violation of this District policy for anyone inside the District to install any wireless device, router, switch or network device that has not been purchased by the District Technology Department.

Infrastructure

All data and telephone wiring, all network switches, all servers, all tape drives, all infrastructure is the sole property of the District, and should not be handled in any physical or electronic way unless authorized by the Superintendent of Schools.

Web Filter

All computers within the District must be filtered when being used on the Internet. Attempts to by-pass the filter or disable it without prior administrative authorization will be a violation of this policy.

Computer Use

The District computers and associated systems are to be used for the educational, administrative and business practice as defined by the District. They may not be used for illegal activity or commercial gain.

The above topics pertain to the integrity of the District's computer systems. Failure to abide by any of the identified procedures and protocols will be considered a breach of this Information Security Policy. The Superintendent of Schools, or his/her appointees, will determine the consequence of violation. Furthermore, the Superintendent of Schools will periodically have the Director of Technology insure that all of the above procedures and protocols are in effect.

Adopted: 8/19/2009