Information Systems Security Standards and Procedures

Davis School District

Related DSD Policy 7SS-001
May 28, 2013

Information Systems Security Standards and Procedures

Davis School District

To ensure the security of the District's information systems the following standards and procedures shall be followed. This applies to all computer and data communication systems connecting or connected to the DSD network.

RESPONSIBILITIES

All users of the District's computer systems and network resources have the responsibility to ensure the overall security of DSD systems and to behave in a manner consistent with this security procedure and the appropriate acceptable use agreement. Each user is responsible for understanding and complying with the appropriate Acceptable Use Agreement and the Information Systems Security Standards and Procedures (*this procedure*) of the District.

1. Ultimate jurisdiction for the security of the District's computer and network systems and information on said systems lies with the Superintendent of Schools.

2. A "Security Team" shall be designated by the Administrator of Technology Services. The Security Team is responsible for all security-related audit activities.

3. All users of the District's network and computer systems are responsible for the security of the District's systems within their realm of responsibilities. Users shall NOT establish their own personal webservers, FTP servers, news servers, electronic bulletin boards, local area networks, wireless access points, modem connections to existing local area networks, or other multi-user systems, such as Peer-to-Peer (PSP), for communicating or transferring information without the specific approval of the Technology Services Department in collaboration with the Security Team.

4. System Administrators have the same user responsibilities listed above plus the additional responsibilities and privileges listed below due to their administrative positions.

   a) System Administrators are expected to keep operating systems and applications current. Where appropriate, all the latest operating system and application patches and updates must be applied.

   b) System Administrators are expected to keep anti-virus software up to date on the systems they administer.

   c) System Administrators are expected to ensure that user information is treated as private. It is recognized that a system administrator may potentially have contact with user files, email, etc., in the course of his or her duties. The contents of such files must be kept private except in cases where said information is a violation of policy, procedure, or law.

   d) System Administrators are expected to participate in security training and other activities provided by the Security Team or designee.

   e) System Administrators are expected to train users on proper security procedures and tactics as directed by the Security Team or designee.

   f) System Administrators are expected to use administration tools, security tools, and audit tools in a professional and ethical way.

SYSTEM SECURITY

This section pertains to all computer and network systems used on the District's network.

1. PHYSICAL SECURITY

a) Network equipment such as servers and routers must be placed in an environmentally controlled location (e.g., temperature control, humidity, exposure to water, etc.).

b) Network equipment should be stored in secure locations (server room, wiring closets, etc.) with restricted access. The data center(s) shall be secured by multiple authentication vectors with access logs for review.

2. USER SECURITY

a) Each District user must login using a unique user ID. System Administrators must be able to uniquely identify all users, including name and user ID.

b) User accounts created for vendors or consultants to provide services must only be active during the time the service is carried out.

c) User accounts will be reviewed periodically to ensure that only valid accounts remain active.

d) All District user accounts must have passwords that comply with the Password Security section of this procedure.

e) System Administrators and all Technology Services staff must never request users to reveal their passwords. If a System Administrator must sign on to a user's account, the password should be reset to give access to the System Administrator for support services. The user must be required to change their password after the support service is completed by the System Administrator.

f) Users accessing District resources or information systems (i.e. Encore or email) from personal devices or devices outside of the District environment must do so in a secure manner as to not allow access to said systems by unauthorized persons.

3. PASSWORD SECURITY

a) Passwords must not be the same as or contain the user ID.

b) Passwords must not be blank or the vendor default. All vendor-supplied default passwords must be changed before any computer, network, or communications system is used.

c) Passwords must contain a minimum of 8 characters, where possible.

d) User must not share passwords with other people. Passwords should remain private.

e) It is understood that passwords needed for system and data administration must be shared with those who administer said systems. Therefore, passwords used for system and data administration should only be revealed on a need to know basis.

f) Passwords must not be written down and left in a place where other people might discover them.

g) Passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized user.

h) Critical system passwords must be changed when a system administrator who knows said system passwords leaves the District.

4. COMPUTER SECURITY

a) Only designated district personnel shall change any of the hardware components of the computer. Tampering with district computers is not acceptable.

b) District owned computers must have and run the most current and updated district approved anti-virus software.

c) Unmanned staff workstations must have the user lock or log off the workstation prior to leaving their computer unattended.

d) All staff workstations must have the auto-lock feature enabled.

e) District approved software and plug-ins should be kept updated and have the necessary patches installed.

f) The District may remove software that may be hindering or degrading the proper use of the computer.

5. DATA SECURITY

a) Sensitive data when in “hard copy” format must be stored only in a locked cabinet or drawer in a room or an area where access is controlled by a lock or card reader or that otherwise has sufficient physical access control measures to prevent unauthorized access.

b) Sensitive data contained in database tables shall be encrypted.

c) Backup data shall be encrypted and stored in a secure manner.

d) Any method or device used for storage that contains sensitive data, passwords, or personal information must be kept in a secure manner. This may include physical security and/or encryption. This includes District and personal equipment.

e) All “hard copy” sensitive data shall be destroyed by shredder and/or incineration when said data is no longer needed in “hard copy.”

f) Sensitive data stored on magnetic media such as hard drives, diskettes, or tapes, must be destroyed or securely erased before disposal.

g) In house applications or web services that require passing personal or sensitive data shall be transferred in a secure manner.

h) Files containing sensitive data stored on shared resources shall have restricted access.

6. NETWORK SECURITY

a) The Security Team may test the security of the network and network attached devices by using vulnerability and exploitation tools.

b) The Security Team may monitor network traffic, device logs, and filter logs to find and mitigate vulnerabilities and exploits.

c) Unused services on network equipment must be disabled (i.e. FTP services running on a non-FTP server).

d) Administration of layer 3 network equipment shall be done using encrypted communication.

e) Administration of layer 2 network equipment should be done using encrypted communication.

7. SERVER SECURITY

a) District approved anti-virus must be installed on all public servers and/or servers that have file sharing enabled.

b) Internet access from servers must be kept at a minimum. External access to internal servers must be approved by an IT departmental administrator in collaboration with the Security Team.

c) Updates/Patches must be applied in a timely manner. Critical patches must be applied as soon as possible.

d) Unused protocols and services must be disabled prior to the server being placed in production environment.

8. INTERNET SECURITY

a) All Internet access shall be filtered and monitored.

b) All users are expected to agree and adhere to the Acceptable Use Agreement before access is given to any network resource or the Internet.

9. MOBILE DEVICE SECURITY

a) Devices running Microsoft operating systems shall have District approved anti-virus installed and running with up to date virus signatures.

b) Mobile devices shall have up to date patches and updates for the operating system.

c) District approved software and plug-ins installed on mobile devices should be kept updated and have the necessary patches installed.

d) Only designated District personnel shall change any of the hardware components of the mobile device outside of normal user uses. Tampering with district mobile devices is not acceptable.

e) All mobile devices assigned to staff must have an auto-lock feature enabled.

f) Any mobile device used for storage that contains sensitive data, directory information, passwords, or personal information must be kept in a secure manner. This may include physical security and/or encryption.

g) The District may remove software that may be hindering or degrading the proper use of the mobile device.

h) The District may employ remote wipe technology to remotely disable and delete any data stored on a District mobile device which is reported lost or stolen.

10. REMOVABLE MEDIA SECURITY

a) Removable media should be scanned by anti-virus and/or anti-malware programs before use on a District computer or server.

b) Removable media that contains DSD sensitive data shall be secured as per the Data Security section of this procedure.

c) Lost or stolen removable media containing DSD sensitive data must be reported immediately.

d) Magnetic media which includes but is not limited to hard drives, diskettes, or tapes, must be physically destroyed before disposal.

e) Non-volatile electronic media storage which includes but is not limited to USB drivers, SD cards or solid state drivers (SSD) must be securely erased or physically destroyed before disposal.

f) Optical media which includes but is not limited to CD or DVD that contains District data shall be destroyed before disposal.

11. EQUIPMENT DISPOSAL/RETIREMENT SECURITY

Equipment (i.e. network switches, routers, access points, etc.) that is no longer being used in service shall be erased or put back to factory default before disposal or retirement.

12. NON-DISTRICT OWNED DEVICES SECURITY

As more people bring non-District owned devices and connect them to the District’s network system, it is imperative for the District to define a section in this procedure to keep the District's information, network and computer systems secure.

a) All devices attempting to connect to District networks must agree and adhere to the Acceptable Use Agreement before access is given to any network resource or the Internet.

b) The District has the right to scan any device attempting to attach to District networks via physical access or District wireless.

c) The District has the right to install or remove District owned software from any device that is attached to District networks.

d) The District has the right to refuse or revoke access to network resources or the Internet.

e) Internet access through the District’s network will be filtered and/or monitored.

SECURITY VIOLATIONS AND MITIGATION

1. ACTIVE VIOLATIONS

Hacking, vandalism, Peer-to-Peer (P2P) software, or other malicious activities are violations of this procedure and are strictly prohibited.

2. INACTIVE VIOLATIONS

These violations are not actively interfering with the integrity of the network or computer system but have the potential to do so. These are typically high risk problems or activities that should be removed from the network or remedied as soon as possible. These violations include but are not limited to:

a) Computer or network systems that the vendors no longer support and have known vulnerabilities or exploits.

b) Applications or software that the vendors no longer support and have known vulnerabilities or exploits.

c) Out of date applications or software that have a patch or update and can be patched or updated but are not.

d) Computer systems that do not have anti-virus or anti-malware protection.

3. MITIGATION

When a security violation is detected the ability to protect network equipment, determine the extent of an intrusion, and recover to normal operations requires corrective actions. The Security Team may mitigate these violations based upon the risk that is posed. These actions may include but are not limited to:

a) Implementing changes to prevent further access to the violation.

b) Isolating the violating systems.

c) Contacting the carrier or ISP in an attempt to stop the attack.

d) Disconnecting the violating systems or the source of the violation.

e) Contacting the police, or other governmental agencies.

f) Shutting down violating systems.

g) Notifying internal managerial and legal personnel.

h) Limit further compromises by disabling accounts, disconnecting network equipment from the network, or disconnecting from the Internet.

i) Accounts and network access may be administratively suspended with or without notice.

ENFORCEMENT OF STANDARDS AND PROCEDURES

Any person suspected of being in violation of this procedure may be referred to law enforcement for prosecution. If that person is an employee of the Davis School District, they may be subject to District disciplinary action which may include dismissal. Violation of this procedure by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of the student.

TERMINATION OF EMPLOYMENT

Upon final implementation of a Personnel Action for termination of an employee all computer access, network access and information systems access shall be disabled or removed immediately. This includes all network systems, VPN access, email, database systems, District websites, web servers, computer systems, and physical access to systems. Data previously generated by terminated employees may be retained for up to 90 days after termination.

DEFINITIONS

“**Acceptable Use Agreement**” is an agreement between the District and users of the District's information systems which states the proper use and expectations of use on the District's information systems.

“**Access”** means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

“**Computer**” means any electronic device or communication facility with data processing ability.

“**Computer system**” means any electronic device or communication facility with data processing ability.

“**Computer network”** means the interconnection of communication or telecommunication lines between computers or computers and remote terminals or, the interconnection by wireless technology between computers or computers and remote terminals.

“**Computer property”** includes, but is not limited to, electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

“**Hacking**” means interfering with, tampering with, or disrupting network or computer resources; Unauthorized attempts to access, accessing, or exploiting computer, network or data resources; Attempting to bypass, disable, avoid or thwart security software, hardware or measures; Gathering of information about user, computer, network or data systems for the purpose of bypassing, exploiting or disrupting said systems.

“**Mobile Device”** includes any computer device that can be described as being transient. Mobile devices include but are not limited to laptops, tablets, smart phones, or other devices that have the ability to connect to the District's network.

“**Removable Media**” means any type of electronic, magnetic, or optical storage device or media. This includes but is not limited to removable hard drives, USB drives, CD/DVD disks, SD cards, solid state drives, or other data storage devices that can be described as being transient.

“**Resources**” means any type of electronic device that can be used by a computer system or utilizes the network or computer systems. This includes, but is not limited to: printers, copiers, facsimile machines, projectors, switches, hubs, routers, network security devices such as firewalls and intrusion prevention systems, wireless access points, servers, phones, and web cameras.

“**Services”** include, but are not limited to, computer time, data manipulation, and storage functions.

“**Software or program”** means a series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results including, but not limited to, system control programs, application programs, or copies of any of them.

“**System Administrator**” means any person responsible for the configuration, maintenance or troubleshooting of the computer or network systems at a school, site, facility or department. Members of the Security Team may also be considered a System Administrator.

“Users” means all students, faculty, staff, consultants, temporaries, volunteers, and others who access the District’s computer network.

Links to AUA Agreements:
Elementary Student Acceptable Use Agreement
Secondary Student Acceptable Use Agreement
Employee Acceptable Use Agreement

Sources: *Utah Code Ann. §§76-6-701 to 705 – Computer Crimes. | DSD Policy 7SS-001 | DSD Policy 7SS-003 | Elementary Student Acceptable Use Agreement | Secondary Student Acceptable Use Agreement | Employee Acceptable Use Agreement*