Washington County School District
121 West Tabernacle Street
Saint George, Utah 84770
435-673-3553

District Policy 3730

Technology Security Policy

Washington County School District - Approved 12-13-16, Revised 12-12-17; Revised 11-14-23

1. Purpose

The purpose of this policy is to ensure the secure use and handling of all District data, computer systems and computer equipment by District students, patrons, and employees.

2. Policy

2.1. Technology Security

It is the policy of the Washington County School District to support secure network systems in the district, including security for all personally identifiable information that is stored on paper or stored digitally on district-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the district, its students, or its employees.

The district will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the district network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of district devices and the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the district's Information Security Officer with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to Washington County School District critically sensitive data. All third party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing our systems or receiving information.

It is the policy of Washington County School District to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and Privacy Act, 20 U.S. Code

§1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Governmental Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

It is also the policy of Washington County School District to fully comply with all applicable FBI Criminal Justice Information Services (CJIS) Security Policy in that all individuals to whom Washington County School District authorizes access to CJIS data shall be subject to CJIS Security Policies.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education. Washington County School District supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect Washington County School District's data, users, and electronic assets.

3. Procedure

3.1. Definitions:

3.1.1. Access: 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.

3.1.2. Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

3.1.3. Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

3.1.4. Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

3.1.5. Computer network: 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.

3.1.6. Computer property: Includes 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.

3.1.7. Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

3.1.8. Encryption or encrypted data: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to

decrypt it.

3.1.9. Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered protected data.

3.1.10. Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

3.1.11. Sensitive data: Data that contains personally identifiable information.

3.1.12. System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

3.1.13. Media: Any physical or digital form containing data. To include but not limited to: paper, floppy disks, optical disks, flash media, hard drives, or any other physical form that is used to store data in any format.

3.1.14. Portable Electronic Media: Any media as defined above that is both an electronic device and is designed to be removed from a computer as part of normal operation. To include but not limited to floppy disks, optical disks, USB flash media, removable flash media (SD cards, Compact Flash, Micro SD, etc) and portable hard drives (standard spinning disk or SSD). Does not include internal hard drives (standard spinning disk or SSD).

3.1.15. CJIS: Criminal Justice Information Services. A division of the United States Federal Bureau of Investigation.

3.1.16. District Owned Device: Any computer system (as defined above) or media (as defined above) that is either owned by the District, leased by the District, loaned to the District, provided to the District in conjunction with standard state operations or a contractual agreement; and the District maintains either direct or indirect control of the device; and the device is subject to Washington County School District policies.

3.1.17. Non-District Owned Device: Any device that does not qualify as a District Owned Device (as defined above).

3.2. Security Responsibility

3.2.1. Washington County School District shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing district-wide IT security, to include development of district policies and adherence to the standards defined in this document.

3.3. Training

3.3.1. Washington County School District, led by the ISO, shall ensure that all district employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all district employees.

3.3.2. Washington County School District, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

3.4. Physical Security

3.4.1. Computer Security

3.4.1.1. Washington County School District shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.

3.4.1.2. Washington County School District shall ensure that all equipment that contains sensitive information will be secured to deter theft.

3.4.2. Server/Network Room Security

3.4.2.1. Washington County School District shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.

3.4.2.2. Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.

3.4.3. Contractor access

3.4.3.1. Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to confirmed directly by the authorized employee who issued the service request or by Washington County School District's Technology Department.

3.4.4. Secure Areas

3.4.4.1. Entryways into secure areas shall remain secure, separated from non-secure areas and access will be controlled by physical security controls.

3.4.4.2. No unauthorized person shall be allowed unescorted access to and in any secure area.

3.4.4.3. Entryways into secure areas will be prominently posted as a secure area.

3.4.4.4. Access Control Lists: Each secure area shall have an access control list that shall document each person whom has access.

3.4.4.5. All persons with authorized access to any secure area shall meet the following requirements:

• Pass a full background check

• Require access to the secure area in order to perform the duties necessary to perform their jobs

• Be approved by the Superintendent, HR Director, or Business Administrator for access into the secure area

• Be documented as approved for access into the secure area on the secure area's access control list

3.4.4.6. Visitor Access

3.4.4.6.1. All visitors will need to produce a Washington County School District identification card, or a government issued identification card before granted access to a secure area.

3.4.4.6.2. Washington County School District shall ensure that visitors will remain escorted by an authorized person listed on the access control list while within a secure area.

3.5. Network Security

3.5.1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

3.5.2. Network Segmentation

3.5.2.1. Washington County School District shall ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.

3.5.2.2. Washington County School District will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

3.5.3. Wireless Networks

3.5.3.1. No wireless access point shall be installed on Washington County School District’s computer network that does not conform with current network standards as defined by the Network Manager. Any exceptions to this must be approved directly in writing by the Information Security Officer.

3.5.3.2. Washington County School District shall scan for and remove or disable any rogue wireless devices on a regular basis.

3.5.3.3. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

3.5.4. Remote Access

3.5.4.1. Washington County School District shall ensure that any remote access with connectivity to the District's internal network is achieved using the District's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be approved by the Director of Technology.

3.6. Access Control

3.6.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

3.6.2. Authentication

3.6.2.1. Washington County School District shall enforce strong password management for employees, students, and contractors.

3.6.2.2. Password Creation

3.6.2.2.1. All server system-level passwords must conform to the Password Construction Guidelines posted on the Washington County School District Technology Website.

3.6.2.3. Password Protection

3.6.2.3.1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential information.

3.6.2.3.2. Passwords must not be inserted into email messages or other forms of electronic communication.

3.6.2.3.3. Passwords must not be revealed over the phone to anyone.

3.6.2.3.4. Do not reveal a password on questionnaires or security forms.

3.6.2.3.5. Do not hint at the format of a password (for example, "my family name").

3.6.2.3.6. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.6.2.3.7. Users must share passwords with direct supervisors or District administration when under an administrative directive to do so and in conjunction with an administrative investigation.

3.6.3. Authorization

3.6.3.1. Washington County School District shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.6.3.2. Washington County School District shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

3.6.3.3. Washington County School District shall ensure that upon employee transfer or termination that appropriate access accounts are modified or suspended.

3.6.4. Accounting

3.6.4.1. Washington County School District shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

3.6.5. Administrative Access Controls

3.6.5.1. Washington County School District shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

3.7. Incident Management

3.7.1. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.7.2. In the event of a suspected or confirmed data breach, Washington County School District shall follow the Washington County School District Data Breach Plan.

3.7.3. Any individual who suspects that a theft, breach or exposure of Washington County School District Protected data or Washington County School District Sensitive data has occurred must immediately contact the District's Information Security Officer.

3.8. Business Continuity

3.8.1. To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations.

3.8.2. Washington County School District shall develop and deploy a district-wide business continuity plan which should include as a minimum:

• Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.

• Secondary Locations: Identify a backup processing location, such as another School or District building.

• Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and

generation of student and employee listings for ensuing a full head count of all.

3.9. Malicious Software

3.9.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

3.9.2. Washington County School District shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.

3.9.3. Washington County School District shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.

3.9.4. Washington County School District shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

3.9.5. All computers must use the District approved anti-virus solution.

3.9.6. Any exceptions to section 3.9 must be approved by the Information Security Officer.

3.10. Internet Content Filtering

3.10.1. Internet Content Filtering is governed by Policy 3700: Acceptable Use Policy.

3.11. Data Privacy

3.11.1. Washington County School District considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

3.11.2. Washington County School District protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (“FERPA”), the Government Records and Management Act U.C.A. §62G-2 (“GRAMA”), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 (“COPPA”) and Utah Administrative Code R277-487 (“Student Data Protection Act”).

3.11.3. Washington County School District shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.11.4. Washington County School District shall ensure that access to CJIS data shall be limited to only those individuals who are authorized.

3.11.5. Protected data shall not be emailed or shared in the cloud with personally owned accounts, except for direct communication with parents and/or guardians containing the specific student records to which they are entitled to.

3.11.6 . As required by the Utah Student Data Protection Act (SDPA), U.C.A. §53A-1-1401 Washington County School District shall follow the District's Data Governance Plan.

3.12. Security Audit and Remediation

3.12.1. Washington County School District shall perform routine security and privacy audits in congruence with the District's Information Security Audit Plan.

3.12.2. District personnel shall develop remediation plans to address identified lapses that conforms with the District's Information Security Remediation Plan Template.

3.12.3. All accounts used to access CJIS data will be audited and verified annually.

3.12.4. Security audits will be documented.

3.13. Media containing sensitive and/or protected data

3.13.1. Washington County School District shall restrict access to media containing sensitive and/or protected data to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.

3.13.2. Washington County School District shall securely store media containing sensitive and/or protected data within physically secure locations or controlled areas.

3.13.3. Disposal of media

3.13.3.1. All media containing sensitive and/or protected data shall be destroyed or wiped using a method that makes the retrieval of data on said media impossible or unrealistic prior to disposal.

3.13.3.2. All media containing CJIS data shall be destroyed consistent with CJIS policy in that:

3.13.3.2.1. Washington County School District shall sanitize, that is, overwrite at least three times digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). Washington County School District shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Washington County School District shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

3.13.3.2.2. Paper copies shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of paper copies shall minimize the risk of sensitive information compromise by unauthorized individuals. Paper copies shall be destroyed by shredding or incineration. Washington County School District shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

3.13.3.2.3. This policy also applies to any printers and/or copiers that have processed CJIS data.

3.13.3.3. Washington County School District shall follow the steps outlined in the Washington County School District Destruction Procedure for Media Containing Sensitive and/or Protected Data.

3.13.4. Media Transport

3.13.4.1. Washington County School District shall protect media containing sensitive and/or protected data during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

3.13.4.2. Controls shall be in place to protect media containing sensitive and/or protected data while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, is the optimal control during transport; however, if encryption of the data isn't possible then Washington County School District shall institute physical controls to ensure the security of the data.

3.13.5. Washington County School District shall ensure that no CJIS data is stored on portable electronic media.

3.14. Non-District Owned Devices

3.14.1. Washington County School District strictly prohibits accessing, storing or transferring CJIS data to non-district owned devices.

3.15. Hosted Applications and Websites

3.15.1. All official websites, to include individual schools and departments shall use web hosting solutions that are officially supported by the Washington County School District Technology Department.

3.15.1.1. Washington County School District recognizes that hosting and maintaining a school website has legitimate educational value for high school students, because of this high schools may apply for an exemption to host their website on their own hardware within Washington County School District's network. All exemptions must be approved by the Information Security Officer.

3.16. Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with the Washington County School District.