Guadalupe Technology Security Policy

1. Purpose

The purpose of this policy is to ensure the secure use and handling of all Guadalupe Agency (hereinafter "Agency") data, computer systems and computer equipment by students, patrons, and employees.

2. Policy

2.1 Technology Security

It is the policy of the Agency to support secure network systems in its programs and Guadalupe School, including security for all personally identifiable information (hereinafter "PII") that is stored on paper or stored digitally on agency-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the Agency, its students, or its employees.

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

This policy and procedure also covers third party vendors and contractors that contain or have access to Agency critically sensitive data. All third-party entities are required to sign the Restriction on Use of Confidential Information Agreement before accessing Agency systems or receiving information.

It is the policy of the Agency 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 Government Records Access and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq. and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in Section 3. 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 Board of Education. The Agency supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect the Agency'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.

3.2. Security Responsibility

3.2.1. The Agency shall appoint an IT Security Officer (hereinafter "ISO") responsible for overseeing Agency-wide IT security, to include development of Agency policies and adherence to the standards defined in this document.

3.3. Training

3.3.1. The Agency, led by the ISO, ensures all Agency 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 Agency employees.

3.3.2. The Agency, led by the ISO, ensures that all students are informed of Cyber Security Awareness.

3.4. Physical Security

3.4.1. Computer Security

3.4.1.1. The Agency's Data Governance Plan ensures that staff computers are not 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 are used to enforce this requirement.

3.4.1.2. The Agency ensures that all equipment that contains sensitive information is secured to deter theft.

3.4.2. Server/Network Room Security

3.4.2.1. The Agency ensures that server rooms and telecommunication rooms are protected by appropriate access control which segregates and restricts access from general school or office areas. Access control is enforced using keys, electronic card readers, or similar method with staff members having only the access necessary to perform their job functions.

3.4.2.2. Telecommunication rooms 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 must present a company issued identification card, and his/her access is confirmed directly by the authorized employee who issued the service request.

3.5. Network Security

3.5.1. Network perimeter controls are implemented to regulate traffic moving between trusted internal (Agency) 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. The Agency ensures that all untrusted and public access computer networks are separated from main Agency computer networks and utilize security policies to ensure the integrity of those computer networks.

3.5.2.2. The Agency utilizes industry standards and current best practices to segment internal computer networks based on the data they contain. This is 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 The Agency's computer network that does not conform to current network standards. Any exceptions to this must be approved by the ISO.

3.5.3.2. The Agency scans for and removes or disables any rogue wireless devices on a regular basis.

3.5.3.3. All wireless access networks conform to current best practices and 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. The Agency ensures that any remote access with connectivity to the Agency's internal network is achieved using the Agency's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

3.6. Access Control

3.6.1. System and application access is 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. The Agency enforces strong password management for employees, students, and contractors.

3.6.2.2. Password Protection

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

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

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

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

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

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

3.6.2. Authorization

3.6.2.1. The Agency ensures that user access is limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.6.2.2. The Agency ensures that user access is granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

3.6.3. Accounting

3.6.3.1. The Agency ensures 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.

3.6.4. Administrative Access Controls

3.6.4.1. The Agency limits IT administrator privileges 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 are designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.8. Business Continuity

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

3.8.2. The Agency developed and deployed a business continuity plan which includes 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.
- 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 ensuring a full head count of all.

3.9. Malicious Software

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

3.9.2. The Agency will install, distribute, and maintain spyware and virus protection software on all Agency-owned equipment.

3.9.3. The Agency ensures that malicious software protection includes 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. The Agency ensures 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 Agency approved anti-virus solution.

3.9.6. Any exceptions to section 3.9 must be approved by the ISO.

3.10. Internet Content Filtering

3.10.1. In accordance with Federal and State Law, the Agency filters internet traffic for content defined in law that is deemed harmful to minors.

3.10.2. The Agency acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, the Agency uses a combination of technological means and supervisory means to protect students from harmful online content.

3.10.3. In the event that students take devices home, the Agency provides a technology based filtering solution for those devices. However, the Agency relies on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

3.10.4. Students are supervised when accessing the internet and using Agency owned devices on school property.

3.11. Data Privacy

3.11.1. The Agency considers the protection of the data it collects on students, employees, and their families to be of the utmost importance.

3.11.2. The Agency 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 Access 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. The Agency ensures that employee records access is limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties is utilized to control authorization access.

3.12. Security Audit and Remediation

3.12.1. The Agency performs routine security and privacy audits in congruence with the Agency's Information Security Audit Plan.

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

3.12.3. Employee Disciplinary Actions are in accordance with applicable laws, regulations, and Agency policies. Any employee found to be in violation of this policy or procedures may be subject to disciplinary action up to and including termination of employment with the Agency.