CYBER SECURITY PLAN

Buffalo Independent School District

PURPOSE

he 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.

REQUIREMENTS

This plan meets the requirements of S.B. No. 820 and is consistent with the information security standards for institutions of higher learning adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code.

Buffalo Independent School District Cyber Security Plan

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

2.1.1. It is the policy of the Buffalo Independent 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.

2.1.2. 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.

2.1.3. 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 Cybersecurity Coordinator with the relevant information.

2.1.4. This policy and procedure also cover third party vendors/contractors that contain or have access to Buffalo Independent School District critically sensitive data.

2.1.5. It is the policy of Buffalo Independent School District to fully conform with all federal and state privacy and data governance laws.

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. Buffalo Independent School District shall appoint a Cybersecurity Coordinator

responsible for overseeing District-wide IT security with duties that include development of District policies and adherence to the standards defined in this document.

3.3 Training

3.3.1. Buffalo Independent School District, led by the Cybersecurity Coordinator, 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.

3.4 Physical Security

3.4.1. Computer Security

3.4.1.1. Buffalo Independent 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.

3.4.1.2. Buffalo Independent 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. Buffalo Independent 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 shall be limited to only IT or other staff members which need access to perform their necessary job functions.

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 be identified, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by Buffalo Independent School District's Technology Department.

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. Wireless Networks

3.5.2.1. No wireless access point shall be installed on Buffalo Independent 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 Cybersecurity Coordinator.

3.5.2.2. 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.

3.6 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. Buffalo Independent School District shall enforce 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. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.6.3. Authorization

3.6.3.1. Buffalo Independent 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. Buffalo Independent 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.

3.6.4. Administrative Access Controls

3.6.4.1. Buffalo Independent 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. The District's Cybersecurity Coordinator shall report any cyber-attack, attempted cyber-attack, or other cybersecurity incident against the district cyberinfrastructure as soon as practicable after the discovery of the attack or incident.

3.8 Malicious Software

3.8.1. Buffalo Independent School District shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops to eradicate malicious software attacks.

3.9 Internet Content Filtering

3.9.1. In accordance with Federal and State Law, Buffalo Independent School District shall filter internet traffic for content defined in law that is deemed harmful to minors.

3.9.2. Buffalo Independent School District acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, Buffalo Independent School District uses a combination of technological means and supervisory means to protect students from harmful online content.

3.9.3. Students shall be supervised when accessing the internet and using district owned devices on school property.

3.10 Data Privacy

3.10.1. Buffalo Independent School District considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

3.10.2. It is the policy of Buffalo Independent School District to fully conform with all federal and state privacy and data governance laws.

3.11 Disciplinary Actions

3.11.1. 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 Buffalo Independent School District.