2000-Operations
400-IT Security Plan

1. **Purpose**
   The purpose of this policy is to ensure the secure use and handling of all Providence Hall Charter School (PHCS) data, computer systems, and computer equipment by PHCS students, patrons, and employees.
2. **Technology Security**
   2.1. It is the policy of PHCS to support secure network systems, including security for all Personally Identifiable Information (PII) that is stored on paper or stored digitally on PHCS-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to PHCS, its students, or its employees. PHCS 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.
   2.2. All persons who are granted access to PHCS network(s) and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of PHCS devices and the network(s). When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the school's IT Manager with the relevant information. This policy and procedure also covers third party vendors/contractors that contain or have access to PHCS critically sensitive data. All third party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing PHCS systems or receiving information.
   2.3. It is the policy of PHCS to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and Privacy Act (FERPA), 20 U.S. Code §1232g and 34 CFR Part 99, the Government Records and Management Act (GRAMA) U.C.A. §62G-2, U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.
   2.4. Professional development for PHCS employees and students regarding the importance of network security and best practices are included in this policy. 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. PHCS supports the development, implementation, and ongoing improvements for a robust security system of hardware and software that is designed to protect PHCS' data, users, and electronic assets.
3. **Definitions**
   3.1. ***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
   3.2. ***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

3.3. ***Computer*** - any electronic device or communication facility that stores, retrieves, processes, or transmits data
3.4. ***Computer System*** - a set of related, connected or unconnected, devices, software, or other related computer equipment.
3.5. ***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
3.6. ***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
3.7. ***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
3.8. ***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
3.9. ***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
3.10. ***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
3.11. ***Sensitive Data*** - data that contains personally identifiable information
3.12. ***System Level*** - access to the system that is considered full administrative access; includes operating system access and hosted application access

4. Security Responsibility

PHCS shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing IT security, to include development of PHCS policies and adherence to the standards defined in this document.

5. Training

5.1. PHCS, led by the ISO, shall ensure that all PHCS employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.
5.2. Training resources will be provided to all PHCS employees
5.3. PHCS, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.
5.4. PHCS students will be trained annually in the procedures outlined in Board Policy (Acceptable Student Use of Internet, Computers, and Network Resources).
5.5. All PHCS employees will be instructed in the procedures contained in Board Policy (Acceptable Employee Use of Internet, Computers, and Network Resources).

6. Physical Security

6.1. ***Computer Security***
6.1.1. PHCS outlines procedures that all employees must take to ensure security on PHCS systems.

6.1.2. PHCS 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 screensaver should be used to enforce this requirement.

6.1.3. PHCS shall ensure that all equipment that contains sensitive information will be secured to deter theft.

6.1.4. PPI should not be stored and transported on any external storage devices.

6.2. *Server/Network Room Security*

6.2.1. PHCS shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or 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.

6.2.2. 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.

6.2.3. Unescorted access to PHCS data center must be approved by the ISO.

6.3. *Contractor Access*

6.3.1. 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 PHCS' IT Department.

7. Network Security

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

7.1. *Network Segmentation*

7.1.1. PHCS shall ensure that all untrusted and public access computer networks are separated from main PHCS computer networks and utilize security policies to ensure the integrity of those computer networks.

7.1.2. PHCSl 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.

7.2. *Wireless Networks*

7.2.1. No wireless access point shall be installed on PHCS' 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 ISO.

7.2.2. PHCS shall scan for and remove or disable any rogue wireless devices on a regular basis.

7.2.3. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA2 AES encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

7.3. *Bring Your Own Device (BYOD)*

7.3.1. Upon signature on acceptable use policy letters, staff, faculty, and students may use personal devices on PHCS' network.

7.3.2. Personal devices are limited to two (2) devices per person on PHCS networks at any given time.

7.3.3. Users may use personal devices to access Internet and Public facing PHCS systems only. No access to internal systems is allowed.

8. Remote Access

8.1. PHCS shall ensure that any remote access with connectivity to the PHCS' internal network is achieved using the PHCS' Remote Access Services.

8.2. The ISO approves all remote access requests.

9. Access Control

9.1. 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.

9.2. Access to systems that contain PPI about students or employees must be authorized by the supervising administrator and reviewed by PHCS IT Department.

9.3. All non PHCS employees (contract workers, volunteers, etc.) requiring access to PII must be authorized by the ISO.

9.4. *Authentication*

9.4.1. PHCS shall enforce strong password management for employees and contractors.

9.4.2. Student passwords will have various forms of complexity commensurate with the student's age, ability, and access to their sensitive information.

9.5. *Password Creation*

All server system-level passwords must conform to the Password Construction Guidelines posted on the Information Systems Department Site.

9.6. *Password Protection*

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

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

9.6.3. Passwords must not be revealed over the phone to anyone. Passwords may be shared over the phone by the PHCS IT Helpdesk to the appropriate person following a verification process.

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

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

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

9.6.7. PHCS will require students and employees to change passwords on regular intervals to protect against unauthorized access.

9.7. *Authorization*

9.7.1. PHCS 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.

9.7.2. Providence Hall Charter School shall ensure that user access should be granted

9.7.3. and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

9.8. ***Accounting***
PHCS shall ensure that audit and log files are maintained 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.

9.9. ***Administrative Access Controls***
PHCS shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

10. Incident Management

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.

11. Business Continuity

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

11.2. PHCS shall develop and deploy a business continuity plan which should include as a minimum

11.3. ***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.

11.4. ***Secondary Locations***:
Identify a backup processing location, such as another school or building.

11.5. ***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.

12. Malicious Software

12.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks.

12.2. PHCS shall install, distribute, and maintain spyware and virus protection software on all PHCS owned equipment, i.e. servers, workstations, and laptops.

12.3. PHCS 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.

12.4. PHCS shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty (30) days and critical patches shall be applied as soon as possible.

12.5. All computers must use PHCS approved anti-virus solution.

12.6. Any exceptions to this section (Malicious Software) must be approved by the IT Manager and/or administration.

13. Internet Content Filtering

13.1. In accordance with Federal and State Law, PHCS shall filter internet traffic for content defined in law that is deemed harmful to minors.

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

13.3. In the event that students take devices home, PHCS will provide a technology based filtering solution for those devices. However, PHCS will rely on parents/guardians to provide the supervision necessary to fully protect students from accessing harmful online content.

13.4. In the event that employees take devices home, PHCS will provide a technology based filtering solution for those devices.

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

14. Data Privacy

14.1. PHCS considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

14.2. PHCS protects student data in compliance with the Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99, the Government Records and Management Act U.C.A. §62G-2, U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 and Utah Administrative Code R277-487.

14.3. PHCS 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.

15. Security Audit and Remediation

15.1. PHCS shall perform routine security and privacy audits in congruence with PHCS' Information Security Audit Plan.

15.2. PHCS personnel shall develop remediation plans to address identified lapses that conforms with PHCS' Information Security Remediation Plan Template.

15.3. Employee disciplinary actions shall be in accordance with applicable laws, regulations, and PHCS policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with the PHCS.