PONCE HEALTH SCIENCES UNIVERSITY

Tamdiu Discendum Est. Quamdiu Vivas

IT Information Security and Privacy Policy

Reason For This Policy

Information Assets and IT Resources are essential to furthering the mission of Ponce Health Sciences PHSU (PHSU). These are PHSU assets, or those entrusted to it by affiliates, that must be protected throughout various phases of their useful life, including when created or collected, stored, transmitted or transferred, and ultimately destroyed. To accomplish this objective, certain administrative, technological and physical safeguards must be in place to adequately protect Information Assets and IT Resources, while supporting their use in furthering PHSU's mission. The Responsibilities outlined in this policy establish and define the organizational structure by which such safeguards are identified, promulgated, implemented and maintained.

Purpose of Policy

A trusted and effective information technology (IT) environment is vital to the PHSU's ongoing mission of discovery, learning and engagement. To this end, PHSU will:

- Establish an overarching Information Security and Privacy Program to establish an environment of internal controls designed to maintain, facilitate and promote adequate protection of Information Assets and IT Resources through standards, procedures, guidelines, information-sharing and training.
- Identify and classify Information Assets and IT Resources according to their use, sensitivity, and importance to PHSU and in compliance with federal and/or state laws.
- Facilitate collaboration and communication among stakeholders throughout PHSU community to aid in protecting Information Assets and IT Resources, with recognition of the need to respond and adapt to rapidly changing and emerging technologies.
- Ensure that access to Information Assets via IT Resources is governed by appropriate role-based access controls and the principles of least privilege PHSU employees being granted access only to those Information Assets and IT Resources they need to fulfill the responsibilities of their position.
- Support the activities and responsibilities of Information Owners, Data Stewards and Data Users within PHSU's IT environment.
- Manage risk to Information Assets and IT Resources through appropriate administrative, technological and physical controls to protect both Information

Assets and IT Resources from unauthorized access or modification, misuse or damage.
- Establish security and privacy controls meeting the requirements of legal, ethical, internally imposed or externally imposed constraints, as required by NIST 800-171, HIPAA, the Gramm Leach Bliley Act (GLB) and other compliance frameworks.
- Establish sanctions appropriate for non-compliance with control standards and procedures or for violation of applicable laws, regulations or other legal requirements.
- Conduct a periodic review of information security standards and procedures to maintain effective controls and relevance to changes in business processes, technology, applicable laws or regulations, and/or problems identified during risk assessments.
- Support, through the maintenance of an effective IT environment and the management of Information Assets and IT Resources for their maximum effective benefit, the PHSU's ongoing mission.

All individuals who use or have access to Information Assets and IT Resources, regardless of the user's role or affiliation with the PHSU, are expected to act in accordance with this policy and its supporting Information Security and Privacy Program, as well as all relevant laws, contractual obligations and the highest ethical standards. Violations may result in disciplinary actions up to and including expulsion or termination or may be referred to appropriate external authorities.

There is a general Privacy Policy is published on PHSU's website.

General Privacy Policy

PHSU carefully protects all nonpublic personal information in our possession regarding students, their families, and employees. PHSU will not release nonpublic, private, personal, or financial information about our students or applicants to any third party, except as specifically provided in this policy. PHSU will release certain nonpublic personal information to federal and state agencies, government contractors, student loan providers/servicers, and other parties as necessary for the administration of the federal student aid programs, for enforcement purposes, for litigation, and for use in connection with audits or other investigations. Disclosure is permitted to law enforcement or emergency services agencies in the performance of their duties or when student safety or health may be in jeopardy. PHSU will not sell or otherwise make available personal information for marketing purposes to any third party at any time.

Protection of Personally Identifiable Information (including PHI)

PHSU employs office procedures, password protection and role-based access to computer systems to ensure the security of paper and electronic records. PHSU does not disclose specifics of its internal security procedures to students or the general public to protect the effectiveness of those procedures.

Access to social security numbers and other Personally Identifiable Information is strictly limited to those PHSU officials with a need-to-know. Each department director is responsible for enforcement of this Policy with regard to the information within their office. The Chief Financial Officer ("CFO") is responsible for overall control of information release and will resolve any disagreements and make final decisions as necessary in accordance with this Policy.

PHSU's information is an important asset that is critical to providing an effective and comprehensive learning environment, openly communicating ideas, providing outstanding community service, and supporting the PHSU's operations and its offering of educational services. This information includes sensitive and personal student, faculty, and staff data as well as the PHSU's operational data. To maintain effectiveness and protect individuals, the PHSU's information assets must be protected from misuse, unavailability, destruction, and unauthorized disclosure or modification. The executive leadership of the PHSU is committed to protecting the value of PHSU's information assets. Its IT Department is charged with establishing and maintaining safeguards to implement a policy that preserves the confidentiality, integrity, and availability of information and information systems. This responsibility is addressed by:

- Continually assessing risks and defining appropriate protection strategies.
- Complying with applicable legal and regulatory requirements.
- Protecting the reputation, image and competitive advantage of the PHSU.
- Supporting PHSU's strategic mission and goals.
- Maintaining partnership with administrative units, faculty, and staff to ensure a collaborative approach to information security.

Policies and procedures provide the foundation of an effective Information Security Program and define minimum requirements for protection of information. The IT Department has developed and implemented technologies that specify appropriate controls and conduct. These technologies have been approved by PHSU's CFO, are applicable to all faculty, staff, and students, and they are required to be followed as follows:

Designation of Representative(s)

PHSU's CFO is designated as the Program Officer who is responsible for coordinating and overseeing this Information Security Program. The CFO may designate other representatives of PHSU to oversee and coordinate particular elements of the Program. Questions regarding implementation or interpretation of the Program should be directed to the CFO or their designee(s). Please note, the definition of a “customer” as used herein is anyone about whom the PHSU collects, views, or keeps any type of financial information. Customers can be students, parents of students (or other relatives), employees, and vendors.

Risk Assessment

The following is a list of potential threats to customer financial information that the Policy is intended to mitigate.

1) Unauthorized access to data through software applications.
2) Unauthorized use of another information system user's account and password.
3) Protection of information at rest and in transit.
4) Resilient operations to recover critical functionality in the event of adverse conditions.
5) Unauthorized viewing of printed or computer displayed student or employee financial information.
6) Improper storage of printed customer financial data information.
7) Improper destruction of printed material that contains student or employee financial information.
8) Appropriate oversight of the security policy.

Consequences

Disciplinary measures for employees, up to and including termination, may be imposed for breaches of the security components of this Policy. Disciplinary measures for students, up to and including termination of enrollment, may be imposed for breaches of the security components of this Program.

Information Systems Management

PHSU’s IT Department is tasked with providing effective security management to prevent, detect and respond to attacks of intrusion, ransomware attacks, social engineering attacks, phishing attacks or other system failures. The IT Department provides the following security measures:

- Provide appropriate antivirus software that can be updated automatically.
- Keep PHSUs electronic information systems updated with patches, new releases, etc., as appropriate.
- Review system architecture and applications for security gaps.
- Backup customer information daily and keep weekly backups off site at a secured location and protected against destruction or damage.
- Allow only approved users access to system components and applications.

- Manage remote access controls.
- Define remote access protocols and protections.
- Notify users about any security risks or breaches.
- When transferring data from one computer to another, erase data from former computer.
- Monitor creation and removal of network assets.
- Monitor use and movement of data stored on protected systems.
- Monitor external threats to system.

Security Policy Monitoring and Testing

This Policy shall be reviewed periodically and adjusted as and when necessary. The most frequent of these reviews should occur within the IT Department, which will monitor software updates and new releases for security software and implement appropriate upgrades and new releases in a timely fashion. In addition, the CFO shall hold such formal and informal meetings with appropriate employees and IT Department staff on an "as needed basis" to review the effectiveness of the Policy and revise as necessary. Any suspected information security breach or issue should be reported immediately to the IT Department.

Version Control

Responsible Office: Office of the Chief Financial Officer

1st Revision Date: September 13, 2021

Original Date Issued: July 1, 2013