To Submit a comment on this draft please click here

University of Pittsburgh
University Information Security Policy

Implementing Executive: Vice Chancellor and Chief Information Officer
Responsible Unit: Pitt Information Technology (Pitt IT)
Category: Administration & Operations
Effective Date: TBD

I. Purpose

The University of Pittsburgh ("University") has a responsibility to minimize security incidents, manage risks, comply with applicable regulations, and uphold the trust of students, faculty, staff, and stakeholders in our institution's handling of its Information assets.

This Policy establishes a comprehensive Information security framework to safeguard the confidentiality, integrity, and availability of data produced, owned, or maintained by the University. This Policy also provides responsibilities for the components of the information security framework that protects Information (i.e., student records, research data, intellectual property, health records, and other Information) in any physical or electronic form.

II. Scope

This Policy applies to anyone who provides or is provided access to educational, research, student, intellectual property, human resource, and other Protected Information in order to process, store, transmit, or manage those Information types at the University of Pittsburgh.

III. Definitions

A. Information - Data the University is responsible for generating, collecting, processing, accessing, transmitting or disposing of in support of a business function.

B. Information Resources - Procedures, equipment, or software used, designed, built, operated, or maintained to collect, record, process, store, retrieve, display, and transmit Information – along with associated personnel including consultants and contractors.

C. Protected Information - Data that has additional safeguards in place in order to control access or use, which is classified as either Restricted or Private per the University's Data Classification and Compliance Standard.

D. Unit - A department, school, office, or other reporting entity of the University that

usually reports to a Responsibility Center (RC) Head.

IV. Policy

The following sections describe the information security framework and provide responsibilities for activities as needed.

A. Access Control, Identification, and Authentication

Access to Information and Information Resources is provided according to the principle of least privilege, which is the application of the most restrictive set of privileges needed for the performance of authorized tasks. Anyone providing access to University Information must ensure that access is granted appropriately to users and in compliance with University Policy and any associated Pitt IT Standards and Procedures. Access control activities may include verifying the identity of users and entities accessing systems and data, typically through passwords, multifactor authorization, biometrics, or other authentication methods. User access must be revoked upon termination of employment, employment responsibility change, separation from the University, or termination of a written agreement granting such access.

For specific restrictions to Information please review the Pitt IT Data Risk Classification and Compliance Standard (and the associated security guides) or contact the Pitt IT Technology Help Desk for consultation before providing access or sharing data.

B. Awareness and Training

Security training is provided by Pitt IT to users to raise awareness of security risks, relevant University Policies, relevant Pitt IT Standards and Procedures, and specific security-related responsibilities and duties. This training must be completed in order to access the University's Information Resources.

C. Audit and Accountability

System activity logging for audits will be performed by Pitt IT to the extent necessary to monitor, analyze, and investigate unlawful or unauthorized system activity. These logs will provide detail of the specific users, systems, and/or processes of activity associated with Univeristy Information Resources, so users as well as those responsible for the relevant systems and/or processes, can be held accountable for those actions.

Activity logging management Information is restricted to users that are responsible for reviewing that activity. Audit logs will be protected from unauthorized access, modification, and deletion.

D. Business Continuity and Disaster Recovery

Business Continuity is an approach to maintaining operations in the event of an unplanned disruption such as a cyber-attack or natural disaster. Disaster recovery is the ability to replicate and back up critical data to a secondary location or multiple locations. Responsibility Centers are required to assess their processes and if needed, develop a plan that documents their business continuity and disaster recovery process.

1. Assessments –The assessment should sufficiently document the reasons for or against the development of a plan.

2. Plans –consist of written procedures for recovering Information systems and business operations in response to a major hardware or software failure, or destruction of facilities. Responsibility Centers are required to review and test plans at least once per year.

E. Incident Response

Pitt IT will maintain an Incident Response Plan that documents the University's detection, reporting, and resolution of cyber security incidents. The incident response plan is developed and reviewed annually, and is supported by Pitt IT, the Office of Risk Management, and the Office of Compliance, Investigations, and Ethics.

F. Information Protection

Information and Information Resources, including physical and digital media, must be protected from unauthorized access and use in accordance with University Policy AO 10, Access to and Use of University Computing Resources, and Pitt IT's Standards and Procedures. The controls set by Pitt IT's Standards and Procedures describe protections during all phases of Information lifecycles. Such protections may include encryption and secure disposal practices.

G. Risk Assessment

The Office of Risk Management will maintain risk assessment processes in consultation with Pitt IT, the Office of Compliance, Investigations, and Ethics and the Internal Audit Department. These processes will be used to assess and manage risks to Information Resources, including the

process for identifying vulnerabilities and details on implementing appropriate safeguards. Pitt IT will issue supplemental Standards and Procedures providing additional parameters around these risk assessment processes in order to ensure security safeguards are in direct proportion to the value of the Information and the Information Resources being protected.

H. Other Components of Information Security

In addition to the elements identified above, Pitt IT will provide Standards or Procedures for the following practices through Pitt IT Standards and Procedures:

1. Configuration Management – Includes establishing, maintaining, and enforcing the use of Information asset inventories and security configuration settings to maintain security and prevent unauthorized changes to them.

2. System Maintenance – The maintenance of systems and equipment as well as controls on the tools, techniques, mechanisms, and personnel conducting maintenance to ensure systems and equipment remain secure and functional over time (i.e., regular updates and patches).

3. Personnel Security – Address security measures related to personnel, including, training, and access control based on roles and responsibilities.

4. Physical Protection – Includes activities and mechanisms/devices that secure physical facilities, equipment, and assets to prevent unauthorized access, theft, or damage.

5. Security Assessment and Monitoring – The process of assessing and monitoring security controls to protect Information assets, determining their effectiveness, and identifying and mitigating deficiencies.

6. System and Communications Protection – Protects the confidentiality, integrity, and availability of Information transmitted over networks and stored on systems.

7. System and Information Integrity – Implements measures to ensure the integrity and reliability of systems and data, including detecting and mitigating vulnerabilities, malicious activity, and unauthorized changes.

8. Planning – Aligns security plans, policies, and procedures with University business goals and assigns parties responsible for developing and implementing them.

9. System and Services Acquisition/Supply Chain Risk Management – Includes processes for acquiring and deploying secure Information Resources, systems, and services, including vendor risk assessments and procurement Standards.

I. Security Control Exceptions

The Chief Information Security Officer (CISO) reviews security control exceptions for the level of university risk and any compensating controls as described by the Responsibility Center Head. Security control exceptions are reviewed annually by the CISO.

V. Noncompliance

Noncompliance with the requirements found in this Policy may lead to removal of access privileges or termination of services through procedures stipulated by Pitt IT, or sanctions as described in the Faculty or Staff Handbooks, or the Student Code of Conduct, as applicable.

VI. Governance or Responsibilities

A. CISO - With the help of Pitt IT, documents, administers, and enforces control activities that support the University's security environment in consultation with other departments (i.e., the Office of Compliance, Investigations, and Ethics; Risk Management).

B. Pitt IT - develops, maintains, and communicates Pitt IT Standards and Procedures that support this policy and provides activities that make up the information security environment. Pitt IT is also a consultative partner to RCs and Units for the implementation of information security activities.

C. RC Heads - Perform Business Continuity/Disaster Recovery assessment and plans as described in IV. D. above.

VII. Contact Information

For questions on the interpretation of this policy please contact the Pitt IT Technology Help Desk at (412) 624-HELP (4357).

For reporting concerns about the information control environment or information control incidents please use the Pitt Concern Connection.

VIII. Related Authorities and Policies

Policy AO 10, Access to and Use of University Computing Resources
Policy AO 11, Computer Data Administration
Policy AO 35, University Administrative Computer Data (UACD) Security and Privacy
Policy CS 30, Health Insurance Portability and Accountability Act (HIPAA)
Policy RI 14, Research Data Management
Pitt IT Data Risk Classification and Compliance Standard

Pitt IT Standards and Procedures