Information Security Policy

Last Modified on 04/24/2025 3:52 pm EDT

For more details about the Information Security Office, **please visit our website**!

1. Introduction

The Wharton School adopts this Information Security Policy to protect the confidentiality, integrity, and availability of digital assets, including information systems that store, process, or transmit data. Wharton shall deploy and use IT resources and services in a manner consistent with the School's research and teaching mission while actively mitigating security risks. This Policy aligns with and adheres to Penn's **IT Security Policy**.

This Policy is a living document that is routinely reviewed and updated to adapt to the evolving Wharton mission, technology advancements, and cybersecurity requirements.

1.1 Purpose and Scope

This Policy directs the establishment of standards, guidelines, and procedures in alignment with the directives of the NIST Cybersecurity Framework (CSF) defined in Section 3.

This Policy applies to all Wharton departments, centers, initiatives, third-party vendors, or affiliates – such as consultants or contractors – authorized to access institutional data, services, and systems. It further applies to all IT systems and services, including data, owned, operated, or maintained by Wharton.

1.2 Compliance

All Wharton employees, students, and contractors are responsible for complying with this Policy and its directives. Wharton's Information Security Office (ISO) will review the Policy and supporting standards annually, updating them based on changes in Wharton's operational environment.

1.2.1 Risk Exceptions

Wharton recognizes that there may be reasons to allow an information technology system to operate outside of the criterion defined in this Policy and related Standards. Exceptions to this Policy may be granted based on a formal, written petition to ISO in adherence to the **Exception Standard**. Approved risk-based exceptions will be documented by ISO, include a defined duration, and be reviewed annually with the goal of achieving compliance.

2. Accountable Stakeholders

2.1 CISO

The Chief Information Security Officer (CISO) leads the Information Security Office (ISO) at Wharton and is accountable for the development and maintenance of security standards, guidelines, and procedures for the School. This role ensures tactical and operational implementations align with the directives established in this Policy.

2.2 Wharton Information Security Office

The Wharton Information Security Office (ISO) oversees the information security and privacy program at Wharton. The team's pillars of success include Information Security Operations & Threat Management, Security Architecture & Engineering, SecDevOps & Application/Product Security, Identity & Access Management, and Governance, Risk, Compliance & Privacy. In partnership with service owners, ISO is responsible for ensuring adequate security and privacy for Wharton.

2.3 Service Owners

Service Owners are designated Wharton staff responsible for overseeing specific systems, applications, or services. Executive Sponsors are accountable for those services. They collaborate with ISO to maintain a secure and resilient digital environment in support of Wharton's mission.

2.4 Wharton Community

Wharton faculty, staff, and students are responsible for adhering to this Information Security Policy. They must comply with security standards and best practices established to support to a safe and resilient digital environment.

3. Security Policy Directives

This Policy directs the establishment of standards, practices, and procedures across the NIST cybersecurity framework pillars: Govern, Identify, Protect, Detect, Respond, and Recover.

3.1 Govern

Program Management

ISO is responsible for overseeing Wharton's information security, privacy, risk, and data governance efforts. This includes measuring compliance with applicable federal laws, regulations, and directives, as well as legal agreements, internal policies and standards.

Risk Management and Assessment

Wharton leverages the Security and Privacy **Risk Review Standard** to assess, identify, and prioritize cybersecurity risks. Risk management techniques must reduce risks to acceptable levels and align with Wharton's strategic objectives. Wharton users are required to review and understand the Data Classification and Governance Standard to ensure awareness of data risk levels and appropriate usage guidelines.

3.2 Identify

Identification and Authorization

Service Owners must ensure users, systems, and processes are uniquely identified and securely authenticated as per the **Identification and Access Management Standard**.

Asset Management

Wharton is required to maintain an inventory of information assets and systems, ensuring their classification and prioritization according to risk and value to the organization.

3.3 Protect

Access Control

Service Owners are responsible for defining access rules and reviewing them annually to ensure proper identification, authentication, and authorization as per the **Identification and Access Management Standard**.

Awareness and Training

ISO provides security awareness and training programs. All Wharton employees will be required to complete training upon request for access to sensitive data and IT systems.

Change Management

Wharton's **Change Enablement Standard** establishes the process for managing changes to IT environments and minimizing risks to system security and availability.

3.4 Detect

Continuous Monitoring

ISO conducts periodic assessments and continuous monitoring of security controls. Identified vulnerabilities must be remediated promptly by the responsible Service Owner and team.

Audit and Accountability

Service Owners are required to process and review audit logs regularly as per the **Audit and Accountability Standard**, ensuring data and services are protected from unauthorized access and tampering.

3.5 Respond

Incident Response

Wharton's **Incident Response Plan** outlines the school's process for handling cybersecurity incidents. The process involves the preparation, detection, containment, eradication, recovery, and post-incident activities. ISO documents, tracks, and reports incidents and conducts periodic tests of the response capability.

3.6 Recover

Contingency Planning

Service Owners are required to align with Wharton's **Business Continuity and Disaster Recovery Plan** in case of system disruption. Systems will be periodically tested to ensure effectiveness.

System and Information Integrity

Service Owners are responsible for identifying, reporting, and remediating system flaws to protect system integrity as per the **Vulnerability Management Standard**.