-->

Security Awareness and Training Standard

Last Modified on 05/18/2026 2:42 pm EDT

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

1. Purpose and Scope

This standard ensures that all individuals accessing Wharton systems and data understand their responsibilities for protecting information and technology assets. Awareness and Training supports a culture of shared responsibility around security and privacy at Wharton to affirm digital trust. This standard is informed by the NIST Cybersecurity Framework (CSF) and aligns with Penn's IT Security Policy and Wharton's Information Security Policy.

This standard applies to all faculty, staff, contractors, vendors, and any individuals or entities accessing Wharton-managed systems, applications, or data. Departments may tailor training to their specific needs, provided the minimum requirements outlined in this standard are met.

2. Definitions

Data Classification: Wharton classifies data based on risk. See the Data Classification and Management Standard for more details.

Security Awareness: General education intended to inform users of basic information security principles and practices applicable to their roles.

Role-Based Training: Security education tailored to the responsibilities of individuals with elevated privileges or access to sensitive data or systems.

Annual Attestation: A yearly confirmation by users and service owners that they have completed required training and understand applicable responsibilities.

Service Owner: Designated Wharton staff member responsible for overseeing a system, application, or service and ensuring compliance with applicable standards.

Training-Required Roles: Individuals whose access to systems, applications, or datasets necessitates specific security training (e.g., administrators, developers, researchers accessing regulated data).

3. Standards

3.1 Security Awareness Program

Wharton must maintain a security awareness program that educates users on their responsibilities for protecting systems and data. The program should promote a culture of informed vigilance and support compliance with Penn and Wharton policies, regulatory requirements, and security and privacy best practices.

3.2 Required Training

All users are required to complete baseline security awareness training (Information Security at Penn: A Practical Guide) within 90 days of onboarding and recommended to complete at least annually thereafter. Departments may supplement baseline training with additional, role-specific content.

3.3 Role-Based Training

Access to systems containing High Risk Data or granting Privileged Access requires completion of specialized training that may cover:

- Data classification and handling practices
- Legal and regulatory obligations (e.g., FERPA, HIPAA, PCI, etc.)
- Government grants (CUI-800-171, 800-53, FERPA, etc.) and organizational contracts with required training
- Secure configuration and system management principles
- Audit and monitoring expectations
- Reporting and responding to security incidents

Service Owners are responsible for identifying roles requiring elevated training and documenting training completion prior to provisioning access.

3.4 Verification and Attestation

ISO will coordinate annual audits to confirm training completion across departments. Wharton departments and service owners must participate in annual attestation of:

- Awareness of this standard
- Compliance with training requirements
- Documentation of training-relevant roles

3.5 Exceptions

Any service or user unable to comply with this standard must submit a formal exception request as per the Exception Standard. Requests must include justification, proposed compensating controls, and an expiration or review date.

4. Roles and Responsibilities

4.1 Information Security Office (ISO)

ISO is responsible for maintaining and updating the security awareness and training program, ensuring its alignment with University policy, legal requirements, and industry standards. ISO provides guidance on training requirements, coordinates periodic audits to verify compliance, reviews and approves training materials, and manages exception requests. ISO also supports departments and service owners in identifying training needs and confirming training completion.

4.2 Service Owners

Service Owners are accountable for identifying which users require security training based on their access to systems or data. They must ensure users complete appropriate training before granting access to services, particularly when High Risk Data or Privileged Access is involved. Service Owners must also maintain documentation of training compliance, make records available upon request, and attest annually to the accuracy and completeness of their training-related responsibilities. Service Owners should consult with ISO to determine appropriate role/system-based trainings.

4.3 Department Leadership

Department leaders are responsible for promoting security awareness within their units and ensuring that staff under their supervision comply with this standard. They play a key role in supporting the implementation of training requirements and participating in annual review and attestation processes coordinated by ISO.

4.4 Service Users

All users are responsible for completing required training in a timely manner, understanding and following Wharton's security practices, and reporting any suspicious or unauthorized activity. Users must not attempt to bypass training requirements or circumvent security controls, and they are expected to operate in accordance with the University's Acceptable Use Policy and other applicable guidelines.

5. Compliance

ISO will compile and provide reporting on adherence to this Standard and related training compliance to senior leadership, including WCIT and HR&PO leadership. Services or departments found non-compliant through risk review or audit may be required to develop a mitigation plan or seek an exception. Users who do not complete required training may be subject to loss of access to Wharton or University systems.