-->

Identity and Access Management Standard

Last Modified on 06/04/2025 2:32 pm EDT

Table of Contents

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

1. Purpose and Scope

The purpose of this document is to establish the Identity and Access Management (IAM) Standard at Wharton. It aims to protect school resources, ensure secure access to systems, and maintain compliance with applicable regulations. In partnership with Penn's IAM Program, this standard supports and enables secure academic, research, and administrative collaboration across the School and University. This standard is informed by University Policies, particularly the University IT Security Policy, Wharton's Information Security Policy as well as best practices detailed in the NIST the Cybersecurity Framework.

This standard applies to all students, faculty, staff, contractors, vendors, and any individuals or entities accessing Wharton systems, applications, or data. Additional requirements must be met for services providing access to any user under the age of 13 or to non-matriculated minors.

This document presumes that any offering has been through a Security Risk Review Assessment as defined by the Security and Privacy Risk Review Standard. Any deviation from this standard will come with recommendations as part of that process on potential alternatives and the risks associated with them.

Top

2. Definitions

The following definitions will cover foundational concepts, local terminology or define general terms to the scope of this document.

- **Authentication:** Verification of identity through credentials.
- **Authorization:** Process of determining user access rights to resources.
- **Coarse-grained Eligibility Population:** A broadly scoped data defined group of University identities used to restrict access through Front-Door Authorization.
- **Fine-grained Eligibility Population:** A data defined group of University identities narrowly scoped to a service or platform used to restrict access through Front-Door Authorization.

- **Front-Door Authorization**: A central Penn configuration blocking the ability to authenticate outside of designated populations. Learn more here: Penn Front Door Authorization.
- **Identity and Access Management (IAM):** Processes and technologies used to manage digital identities and control access to resources.
- **Information Security Office (ISO):** Wharton's Information Security Office, owners and maintainers of this standard.
- **Least Privilege:** Providing the minimum level of access necessary to perform a task or role.
- **Multi-Factor Authentication (MFA):** An enhanced security control for authentication that requires users to provide multiple verification factors. Sometimes called Two-Step or Two-Factor Authentication (TFA).
- **Platform:** A Platform is defined as a service or collection of services that makes use of shared credentials and/or process.
- **PennCommunity:** Penn employee biographic, demographic, and affiliation information.
- **PennGroups:** University managed authorization service. Closely coupled with PennKey SSO.
- **PennID:** An immutable and unique identifier associated with a PennKey.
- **PennKey:** An individual's username and an associated password within the PennKey authentication system. A PennKey is required to authenticate your identity to access many of Penn's online resources.
- **PennName:** A PennName is the username associated with your PennKey.

PennNames may contain mutable Identity information, such as last names, and may be subject to change. A PennName once used is no longer available for reassignment.

- **Privileged Access**: Privileged access is any permission within a service that is not inherent in access to the service.
- **Human Resources & People Operations (HR&PO):** Primary Wharton business stakeholder for IAM policies and process.
- **Service:** Any product, tool or offering into which users are populated and/or for which access is limited or granted based on the user connecting.
- **Service Owner:** Designated Wharton staff responsible for overseeing specific systems, applications, or services.
- **Single Sign-On (SSO):** Is an authentication workflow that allows for a single interactive authentication to work across a series of services sharing the same configuration for a length of time.
- **Two-Step Authentication:** an alternate term for MFA and used at the School level to refer to Penn's implementation of MFA with PennKey and Duo.

Top

3. Standards

3.1 Identity Management

Each authenticated service grants access based on an established identity. The identity must have agreed upon identity verification processes. The strenuousness of identity verification increases based on the sensitivity of the data and/or the impact of the service involved.

PennKey is appropriate for use as part of the controls around systems providing data of any classification.

All services should make use of PennKey for identity verification.

3.1.1 Holds

Services storing data and/or communications must maintain a process for preserving and optionally exporting said data or communications. Hold process must be documented.

3.1.2 PennName Changes

Upon a change to a PennName service owners must handle such changes and do so in a timely manner. Ideally this is done without additional request by the user and is defined by central identity services (Penn Community). Verification of new PennNames should be done by insuring continuity of PennID.

3.2 Authentication

3.2.1 Interactive Authentication

Interactive Authentication is the process by which a user logs in to a service and is prompted to enter/provide credentials. All services must include multiple factors (MFA/Two-Step verification).

All services should make use of PennKey for authentication and require Two-Step verification for the account. When PennKey is not suitable, service owners must establish the methodology for authentication and provide to ISO as directed by the Security and Privacy Risk Review Standard. The service must create and maintain documentation and process for the agreed upon authentication model.

PennKey Single Sign-On (SSO) allows for an existing browser session to grant access without requiring an additional interactive authentication request and must be used for web applications and Software as a Service (SaaS) offerings.

3.2.2 Delegated Authentication

Some services allow for authenticating as users outside of the interactive login flow. This is normally accomplished through a client-level token authorized after an initial interactive authentication and is often in place for mobile apps, or for local application clients. Services leveraging these tokens must document the process by which they are managed and ensure they reflect current status of the user account. Any difference in handling of delegated authorization from interactive authorization must be reviewed by ISO as directed by the Security and Privacy Risk Review Standard. The service must create and maintain documentation of the agreed upon controls for delegated authorization.

3.3 Authorization and Access Control

Authorization determines the access available to a given identity following a successful authentication. To meet operational and business requirements, authorization needs to be able to be revoked and granted in a timely manner.

All services should make use of central Penn Authorization services (SailPoint IIQ or PennGroups) for authorization purposes.

Where possible SSO applications should make use of and document use of Front-Door authorization and document the Coarse-grained or Fine-grained Eligibility Population that restricts authentication.

3.3.1 Platform Access

Services must document criteria for users gaining and losing access. Documentation should include specifics around allowing/denying Alumni, Students, Faculty, Staff and External Users. Any further restriction, such as a specific relationship with Wharton, should also be documented.

Services must have established and documented criteria and process for authorized agents, including ISO, to revoke access to the platform on an agreed upon timeline based on business or legal requirements.

The service must create and maintain documentation of the agreed upon Platform Access components.

3.3.2 Privileged Access

Services must document all privileged access along with the criteria for that access in the service. Services must have established and documented criteria for authorized agents, including ISO, to revoke privileged access on an agreed upon timeline based on business or legal requirements. The principals of least privilege should be used for establishing any elevated access within a service.

Accounts granted privileged access must have MFA configured.

3.4 Monitoring and Auditing

Services are responsible for tracking all successful and failed authentication attempts. Service owners must make these logs available to the Wharton Information Security Office. At a minimum these logs must include the attempted username, originating IP address and timestamp.

Any administrative actions must also be logged and likewise made available.

Service owners should review and attest to ISO at least quarterly that only authorized users have access to the platform, and that authorization is accurate to documented service definitions.

3.5 Incident Response

Unauthorized access of an account or access to resources that are not explicitly approved constitutes a security breach and a violation of University Policy. The Information Security Office must be notified as soon as such behavior is identified or presumed. The Information Security Office will assist with review and classification of the behavior as well as establishing the legal and University responsibilities in the event of a breach.

The Information Security Office must be provided a documented and agreed upon process to revoke platform and/or privileged access or otherwise isolate an account in the event of notification of a breach.

3.6 Training and Awareness

Services that grant access to data or resources that are subject to specific regulation, policy or otherwise requiring specific training must verify directly or receive an assertion that the training is complete. The list of appropriate

trainings should be documented.

3.6.1 Documentation

All documentation required by this standard must be made available to ISO and other appropriate stakeholders and be confirmed by those parties to contain sufficient information for fulfillment of responsibilities. This documentation must be operationally maintained and reviewed at least annually by the service owner.

Top

4. Roles and Responsibilities

4.1 Information Security Office

On behalf of the Wharton School the Information Security Office is responsible for:

- Assessing changes in University Policy, regulation, and community best practice to inform this standard and reviewing the standard annually.
- Measuring and pursuing compliance for the catalog of services hosted or managed by the school.
- Establishing IAM strategies to meet business needs that fit within operational capacities of the school and facilitate continuous improvement.
- Identifying IAM technology needs and solutions in use at the school and aligning them with strategy.
- Clarifying and optimizing overall IAM process at the Wharton School and as part of the University community.
- Coordinating mitigations for IAM related concerns that bridge multiple service offerings at the Wharton School.

For individual services ISO is responsible for:

- Consultation in the event of an incident causing a service to fall out of compliance with this standard or the services documented service targets. The Information Security Office will assist in identifying remediation in line with University Policy, legal regulation and community best practice for such incidents.
- Revocation of platform access and/or privileged access based on business need or legal requirements.
- Processing holds as requested by University General Council and/or additional entities designated in service definitions.
- Providing IAM architectural recommendations and reviews on request.
- Authorization of any deviation from this standard by according to the Exception Standard.

4.2 Wharton Computing

Wharton Computing will provide operational management of appropriate IAM related tools hosted by the School in consultation with the Information Security Office. Wharton Computing is also a key stakeholder in reviewing operational burdens of hosted tools.

4.3 Wharton Human Resources & People Operations

HR&PO are key stakeholders in defining business requirements and principal invokers of IAM processes. HR&PO are responsible for defining the criteria that associate University Faculty and Staff with the Wharton School. As principal invokers HR&PO will be the drivers of the requests for managing changes to a faculty or staff members identity and access based on official status changes in University systems of record for non-student populations.

4.4 Wharton Senior Vice Dean of Teaching and Learning

The Senior Vice Dean of Teaching and Learning is a key stakeholder in defining academic business requirements. Specifically in establishing the criteria that associate University Students with the Wharton School and its academic programs.

4.5 Service Owners

Service Owners are accountable for adherence of their service to this standard.

Service Owners are responsible for:

- Identifying, documenting and maintaining the Identity and Access Management processes supporting their service.
- Asserting the accuracy of service IAM documentation at least annually.
- Consulting with the Information Security Office in the event their process falls out of compliance with this standard and/or the documented configuration for their service.
- In the event of unauthorized access to their service, service owners must ensure that such activity is reported to the Information Security Office immediately.

4.6 Service Users

Users of a service are responsible for only taking actions appropriate to the intended use of the service. Users are responsible for not sharing their credentials or for otherwise providing access to a service or the resources it makes available in a manner that bypasses authorization controls. Users are responsible for being aware of and adhering to the University Acceptable Use Policy on Electronic Resources and other relevant policies.

Top

5. Compliance

ISO will compile and provide reporting on adherence to this Standard and related policy to key leaders and stakeholders in the institution including the COO/CFO, CIO, CISO and the Executive Director of Human Resources and People Operations.

Services that do not meet an acceptable level of compliance through a Risk Review Assessment will be required to receive a formal Exception. Absent a formal exception, services will be requested to be taken offline until suitable mitigations or alternative services are available.