-->

Data Classification and Management Standard

Last Modified on 06/26/2025 4:34 pm EDT

Table of Contents

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

1. Penn Data Classification

The Penn Data Classification framework categorizes university data into three levels based on sensitivity and potential impact if exposed or misused. However, Wharton refines the Moderate Risk category into two distinct subcategories to ensure appropriate security controls, particularly for personally identifiable information (PII) and regulated data. This framework is grounded in Wharton's Information Security Policy, which outlines the principles and responsibilities for securing institutional data.

The classification levels are:

Classification	Low	Moderate (Non-PII / Non-FERPA)	Moderate (PII and/or FERPA)	High

Classification	Low	Moderate (Non-PII / Non-FERPA)	Moderate (PII and/or FERPA)	High
Definition	1. The data is intended for public disclosure, OR 2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the University's mission, safety, finances, or reputation and the loss would have no adverse impact on any individual.	1. The data is not generally available to the public. 2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the University's mission, safety, finances, or reputation or the loss would have a mildly adverse impact on any individual.	1. The data is not generally available to the public. 2. The data includes Personally Identifiable Information (PII) or FERPA-regulated student records which is protected by law/regulation. 3. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the University's mission, safety, finances, or reputation or the loss would have a mildly adverse impact on any individual.	1. Protection of the data is required by law/regulation and Penn is required to report to the government and/or provide notice to the individual if the data is inappropriately accessed. 2. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the University's mission, safety, finances, or reputation or the loss would have a significant adverse impact on any individual.
	• PennKey username • PennID • Publicly available Penn website content • Public university policies • Job postings • University directory	• Non-public Penn policies and manuals • Non-public contracts without sensitive content • Internal Penn emails, budgets, and financial plans that do not contain High-Risk data • Engineering,	• Student education records and admissions applications (excluding K-12 student records) • University directory information not designated for public view • Unpublished research data that	• Health Information, including PHI • Mental health records • Biometric data (e.g., DNA, fingerprints) • PennKey passwords and system credentials • Health Insurance policy ID numbers

Classification	Low information designated for public view	Moderate design, and operational data regarding Penn infrastructure	High contains PII or FERPA-covered records	High • Social Security Numbers • Credit card and financial account numbers
Examples of Data	• Publicly available research data	**(Non-PII / Non-FERPA)** • Unpublished research data (not including PII or FERPA data) • De-identified data • Penn proprietary data (including code) • Non-Penn contract/Data Use Agreement data	**(PII and/or FERPA)** • Operational data that includes limited PII (e.g., student ID numbers without other identifying details)	• Location data that tracks individuals • Export-controlled research data • Driver's license or government-issued ID numbers • Passport or visa numbers • HR records (salary, performance, discipline) • Donor records and non-public gift information • K-12 student records and data related to minors • Hazardous materials and security information

Top

2. Security Controls by Classification

Security controls are measures required to protect university data based on its classification level. Wharton security controls align with university-wide policies, the NIST Cybersecurity Framework, and industry best practices to ensure appropriate safeguards.

Note: The controls listed here represent baseline requirements for each classification level. **They are not exhaustive.** Additional security measures may be necessary based on the specific context or risks associated with a given initiative. A formal risk review should be used to evaluate and determine any supplementary requirements. For more details, see Wharton's Risk Review Standard.

Low	• **No authentication required** (data is intended for public access). • **Public access permitted** via university websites or public repositories. • **Regular system and data backups** to recover from accidental loss or corruption. • **Basic integrity checks** to ensure data is not altered unintentionally. • **Monitoring for availability** to ensure public resources remain accessible. • **Vulnerability and accessibility scans** to maintain publicly available web content. • **Security event logging and monitoring** of access with at least IP, username and timestamp.
Moderate (Non-PII / Non-FERPA)	• **PennKey and multi-factor (MFA) authentication required** to access data. • **Role-Based Access Control (RBAC)** ensures appropriate active university affiliations. • **Encryption in transit and at rest** (e.g., HTTPS, TLS) to protect data from interception. • **Access limited to appropriately protected interfaces or endpoints** compliant with university policy • **Regular system and immutable-data encrypted backups** to recover from accidental loss, corruption or compromise. • **Basic integrity checks** to ensure data is not altered unintentionally. • **Monitoring for availability** to ensure internal resources remain accessible. • **Security awareness training** for employees handling moderate-risk data. • **Security event logging and monitoring** of access with at least IP, username and timestamp. • **Regular vulnerability scans** to identify and remediate security risks. • **Incident response procedures** in place to respond and notify on potential breaches or unauthorized access.

Moderate (PII and/or FERPA) These additional security controls are required in addition to the standard Moderate data requirements.	• **PennKey and multi-factor (MFA) authentication required** to access data. • **Role-Based Access Control (RBAC)** ensures only authorized roles have access. • **Encryption in transit and at rest** (e.g., AES-256, TLS 1.2+) to protect data from interception. • **Access limited to appropriately protected interfaces or endpoints** compliant with university policy • **Regular system and immutable-data encrypted backups** to recover from accidental loss, corruption or compromise. • **Basic integrity checks** to ensure data is not altered unintentionally. • **Monitoring for availability** to ensure internal resources remain accessible. • **Security awareness training** for employees handling moderate-risk data with FERPA/PII. • **Security event logging & monitoring** (e.g., SIEM tools) inclusive of IP, username, timestamp, authorization changes and privilege escalation. • **Audit logging must be exported from source systems to an ISO-specified solution**. These audit logs must include authorization and activity logs and, for interactive sessions, include PennKey username and IP address. These logs must contain any service specific requirements as detailed in an ISO risk disposition. • **Continuous security monitoring & threat detection** (SIEM tools, anomaly detection, vulnerability scanning) and dedicated staffing. • **Data retention policies** enforce proper deletion or anonymization of student/PII data after the required period. • **Data Loss Prevention (DLP) controls** to prevent unauthorized transfers of PII and FERPA data. • **Regular security audits and risk assessments** to ensure compliance with regulations and institutional policies. • **Incident response procedures** in place to respond and notify on potential breaches or unauthorized access. • **Secure data disposal practices** (shredding, secure deletion tools) to prevent data leaks.
	• **PennKey and multi-factor (MFA) authentication required** to access data. • **Role-Based Access Control (RBAC)** ensures only authorized individuals in appropriate roles have access.

High	• **Encryption in transit and at rest** (AES-256, FIPS-compliant encryption) to meet required specifications. • **Access limited to appropriately protected interfaces or endpoints** compliant with university policy • **Regular system and immutable-data encrypted backups** to recover from accidental loss, corruption or compromise. • **Basic integrity checks** to ensure data is not altered unintentionally. • **Monitoring for availability** to ensure internal resources remain accessible. • **Security awareness training** for employees handling high-risk data and relevant compliance requirements. • **Security event logging & monitoring** (e.g., SIEM tools) inclusive of IP, username, timestamp, all create, read, update and delete activity. • **Audit logging must be exported from source systems to an ISO-specified solution**. These audit logs must include authorization and activity logs and, for interactive sessions, include PennKey username and IP address. These logs must contain any service specific requirements as detailed in an ISO risk disposition. • **Continuous security monitoring & threat detection** (SIEM tools, anomaly detection, vulnerability scanning) and dedicated staffing. • **Data retention policies** enforce proper deletion of high-risk data after the required period. • **Data Loss Prevention (DLP) controls** to prevent unauthorized transfers of protected data. • **Regular security audits and risk assessments** to ensure appropriate compliance aligned with data classification and institutional policies. • **Incident response procedures** in place to respond and notify on potential breaches or unauthorized access. • **Secure data disposal** practices (shredding, secure deletion tools) to prevent data leaks. • **Regular penetration testing** to identify and remediate security risks. • **Annual compliance assessments** (HIPAA, PCI-DSS, FERPA, ITAR, CUI, FISMA, FEDRAMP) to ensure regulatory adherence.

Top

3. Associated Services

Wharton provides a range of IT tools and platforms that support various data types based on their classification. Though scope changes, integrations, and initiatives leveraging these tools still require a review, some examples

include:

Low	Moderate (Non-PII / Non-FERPA)	Moderate (PII and/or FERPA)	High
• Public university websites • Campus maps • Public research repositories • Research data pulled from publicly available websites (no DUA in place) • Wharton Share Drive • Non-managed endpoints (e.g. laptops, desktops, public computers, etc.)	• Private university websites (restricted) • Penn O365 • SharePoint (non-sensitive documents) • Zendesk/Halo • Microsoft Teams (non-sensitive) • Slack (general discussions) • Microsoft Azure • Google Cloud Platform • BitBucket • Penn GitHub • Atlassian Suite (Jira, Confluence, OpsGenie, etc.) • Penn SmartSheet • Wharton/Penn Qualtrics • Wharton Google Workspace • Wharton-managed endpoints (e.g. laptops, desktops, public computers, etc.)	• Canvas • Internal data repositories with student or faculty PII • Dropbox • Penn Box • Penn Warehouse • Penn Zoom • Salesforce • Wharton/Penn Amazon Web Services (AWS) • Wharton-managed Servers • ChatGPT Edu • Grammarly • Panopto • Microsoft Copilot Chat	• Workday (HR and payroll data) • Research databases with PHI or SSN • Federal/State grants/DUA and CUI, FISMA, FERPA • Cybersource • PennCommunity • Salesforce (Donor Records) • Salesforce (Global Youth) • BenFinancials • Concur • Microsoft 365 Copilot Chat