-->

Information Security Glossary

Last Modified on 06/01/2026 11:19 am EDT

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

Information Security Terms and Acronyms

Information security terminology can often be highly technical and filled with acronyms that may be unfamiliar to faculty, staff, students, and third-party partners. This glossary is intended to provide clear, accessible definitions for commonly used information security, privacy, and technology terms referenced in Wharton and University security guidance.

The definitions below are designed to support a shared understanding of security concepts used in risk reviews, system architecture discussions, compliance activities, and day-to-day technology operations.

Common Information Security Terms

Access Control

The process of restricting access to systems, applications, or data based on a user's identity and authorized permissions.

Authentication

The process of verifying the identity of a user, system, or application before granting access.

Authorization

The process of determining what an authenticated user is permitted to access or perform within a system.

California Consumer Privacy Act (CCPA)

A California privacy law that grants consumers rights regarding how businesses collect, use, share, and manage their personal information.

Confidential Data

Information that requires protection from unauthorized disclosure due to legal, regulatory, contractual, or institutional requirements.

Data Classification

The process of categorizing data based on its sensitivity and required level of protection.

Data Flow Diagram

A visual representation of how data enters, moves through, is stored within, and exits a system or application environment.

Electronic Protected Health Information (ePHI)

Protected Health Information (PHI) that is created, stored, transmitted, or received electronically.

Encryption

The process of converting information into a protected format that can only be accessed using an approved decryption method or key.

Firewall

A security control that monitors and restricts network traffic between systems or security zones based on defined rules.

General Data Protection Regulation (GDPR)

A European Union privacy regulation that establishes requirements for the collection, processing, protection, and transfer of personal data belonging to individuals located in the European Economic Area (EEA).

Gramm-Leach-Bliley Act (GLBA)

A U.S. federal law that requires financial institutions to protect customers' nonpublic personal information and maintain safeguards to ensure the confidentiality and security of that information.

Health Insurance Portability and Accountability Act (HIPAA)

A U.S. federal law that establishes requirements for protecting the privacy and security of health information and governs the use and disclosure of Protected Health Information (PHI).

Least Privilege

A security principle in which users and systems are granted only the minimum level of access necessary to perform required functions.

Multi-Factor Authentication (MFA)

An authentication method requiring two or more verification factors to gain access to a system or application.

Payment Card Industry Data (PCI Data)

Information associated with payment card transactions, including credit card and debit card data, that must be protected in accordance with Payment Card Industry (PCI) security requirements.

Personally Identifiable Information (PII)

Information that can be used to identify an individual, either directly or indirectly.

Protected Health Information (PHI)

Individually identifiable health information that relates to a person's health condition, healthcare services, or payment for healthcare and is protected under HIPAA.

Risk Assessment

A process used to identify, evaluate, and document potential security risks to systems, applications, or data.

Sarbanes-Oxley Act (SOX)

A U.S. federal law that establishes financial reporting, recordkeeping, and internal control requirements for publicly traded companies to help ensure the accuracy and integrity of financial information.

Security Incident

An event that may compromise the confidentiality, integrity, or availability of information or systems.

Single Sign-On (SSO)

An authentication capability that allows users to access multiple applications using a single set of credentials.

Risk Review

A review process used to evaluate the security posture and risk associated with third-party products, services, or providers.

Common Acronyms

Acronym	Definition
ACL	Access Control List
API	Application Programming Interface
DNS	Domain Name System
EDR	Endpoint Detection and Response
IAM	Identity and Access Management
IP	Internet Protocol
MFA	Multi-Factor Authentication
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
SaaS	Software as a Service
SIEM	Security Information and Event Management
SSO	Single Sign-On
TLS	Transport Layer Security
VPN	Virtual Private Network