University of Wisconsin-Stevens Point
Information Technology

Common Definitions

Date Drafted: 7/15/2008
Date Approved: 02/02/2009
Date Revised:

Status	Responsible University Office
☐**Draft**	Information Technology
☐ **Under Review**	
☑ **Approved**	**Responsible Coordinating Office**
☐ **Obsolete**	Information Technology

1. Purpose

This document provides a set of terms and definitions to ensure that common language and definitions are applied for all IT policies, procedures, references, standards, and guidelines.

2. Terms and Definitions

Access (to data): The capacity to enter, modify or delete data or the capacity to view, copy or download data.

Application Server*:* The computer hosting the application to which the general end-user or the point of-sale (POS) terminal connects**.**

Authorized Requesters: Unit heads or individuals with delegated authority to authorize and initiate access requests in accordance with procedures established by unit heads or higher-level management in their organizational reporting chain.

Business Associate Agreement: A requirement of the Health Insurance Portability and Accountability Act (HIPAA) privacy regulation to have written agreements which apply to any uses or disclosures of PHI (see definition below) data.

Chief Data Stewards: Senior administrative officers of the University responsible for managing information resources while conducting University business. The Provost and Vice Chancellor for Academic Affairs and the Senior Vice Chancellor for Administration and Finance are the Chief Data Stewards of University data.

Confidentiality: Preventing the disclosure of information to any person not authorized to view, copy, or distribute that specific information.

Data Administrator: Technical contact that has operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information. This includes the installation, maintenance, and operation of computer hardware and software platforms. The data administrator may or may not be an employee of Information Technology.

Data Domain: The entire collection of data for which an institutional employee functioning as a data steward or data coordinator is responsible. The data domain also includes rules and processes related to the data.

Data Governance: The quality control discipline for assessing, managing, using, improving, monitoring, maintaining, and protecting institutional data. It is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.

Data Stewards: Registrar, Controller, Director of Personnel and Payroll Services, Deans, Vice-Chancellors, Associate Vice-Chancellors, or others identified by the Chief Data Stewards to manage a subset of data (i.e., they are responsible for its accuracy, integrity, and implementation of policy and procedures for appropriate use of the data).

Data Users: Individuals who are authorized to access University data in the performance of assigned duties, typically employees of the University or contractors**.**

DOD-level wipe**:** United States Department of Defense level sanitization standards for deleting all information from a computer hard drive.

Employees: Faculty and Academic Staff (as defined by the Faculty Handbook), Classified Staff (as defined by the Classified Employee Handbook),visiting faculty from other educational institutions, guest lecturers, contractors, personnel from third parties on temporary assignment, and student employees.

Encryption: Using programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key – usually a user-selected key.

Filter: The process of examining a file or content acquired through the network or from media (e.g. CD or diskette) for harmful or malicious content.

Firewall: A device or program designed to control the network traffic allowed to flow to a computer or segment of the network.

Information Security Office: Under the general direction of the CIO, the Information Security Officer (ISO) is responsible for the development and delivery of an information security and privacy program for the university. The ISO typically works with a security team directing implementation of institutional data access and protection policies and procedures.

Information Technology Resources: Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.

Institutional Data: Any data needed to conduct operations of the university.

Integrity: The amount of confidence that the information has not been modified in an unauthorized or incorrect way.

Intrusion Detection System (IDS): A network or workstation-based system used to detect and notify critical individuals when an intrusion attack is happening.

Intrusion Prevention System (IPS): a network-based ID that can automatically react and prevent attacks from successfully occurring. Special care must be taken with IPS to ensure that the system does not prevent communication that should occur, even during attacks.

Payment Card Industry Data Security Standard (PCI DSS): a multifaceted security standard that includes requirements for security management, policies, procedures.

Phishing: Sending a spam email message which notes an event requiring the receiver to directly provide personal information or inviting the receiver to go to a specially crafted website to provide personal information that will be used for fraud.

Protected Health Information (PHI): Under HIPAA, includes any individually identifiable health information. PHI is personal, identifiable information about individuals which is created or received by a health plan, provider or health care clearinghouse. It includes identifiers such as name, address, birth date, social security number and health plan beneficiary number.

Reliably erase – A process used to assure that data is destroyed or removed from a storage device. This can be achieved by the proper use of specialized software programs that overwrite the data so that it is unrecoverable. This cleaning process is also known as "sanitizing" or "wiping".

Sensitive data - any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Contact Information

For questions about this reference document or Information Technology policies and procedures, contact the Director of Information Technology/CIO.