WSU Information Security Roles, Responsibilities, and Definitions

OVERVIEW

Information security roles, responsibilities, and definitions enable effective communications by providing clarity, alignment, and defining expectations to those executing the work. A common lexicon is needed to share a common understanding and ensure consistency among related and dependent terms.

This section supports Executive Policies EP37: WSU Information Security Policy and EP8: University Data Policies.

Purpose

This section (*BPPM* 87.01) articulates:

- Specific roles and responsibilities and definitions with respect to WSU workforce members, their work, and the information security policy (EP37) and the data policies (EP8), and
- Defines terms that are important to information security management for WSU workforce members, data, systems, and software.

Scope

This policy applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, transmit, or share institutional data.

ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply to implementation of the University's Information Security Policy (EP37) and the University Data Policies (EP8).

Authorizing Official (AO)

An authorizing official (AO) is an executive head of a major institutional business unit or other senior University official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations.

Chief Information Officer (CIO)

The CIO is the University official who is accountable for and is authorized to establish and maintain a University-wide Information Security and Privacy Program, and to authorize publication of the information security and privacy related policies, standards, and guidelines necessary to ensure the confidentiality, integrity, and availability of institutional data and systems.

Chief Information Security Officer (CISO)

The CISO is the University official responsible for establishing and maintaining WSU's enterprise-wide information security and privacy management program for the purpose of appropriately protecting WSUs information and technical assets.

WSU Information Security Roles, Responsibilities, and Definitions

CISO (cont.)

The CISO is the Chief Information Officer's primary liaison to work with senior management and staff across the University to:

- Implement practices that meet defined policies, standards, and regulatory requirements for information security and privacy;
- Determine information security and privacy risk classifications; and
- Drive information security and privacy objectives into business systems and processes throughout the University.

Data Custodian

A data custodian is a University administrator who is assigned by and accountable to an information owner. A data custodian has administrative and/or operational responsibility over specific institutional data sets delegated to them by an information owner. These individuals are responsible for facilitating, implementing, and enforcing institutional data policies, standards, and procedures established by the University and/or the information owner.

System Administrator

A system administrator is the individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information assurance policy and procedures.

Data User

A data user is any University employee, student, individual, affiliate, or third party who is authorized to access institutional systems and data.

Information Owner

An information owner is an executive head of a major institutional business unit (e.g., vice president, chancellor, or dean) reporting directly to the President or Provost. An information owner is accountable for the stewardship of institutional data within their area of responsibility. They are responsible for ensuring the information security and privacy of institutional data, to include its creation, collection, storage, processing, transmission, usage, access, release, maintenance, and disposal.

An information owner may delegate these administrative duties to one or more University administrators known as data custodians for specific institutional data sets or functional areas. The information owner, however, retains ultimate accountability, to include when data is shared or released to third parties.

WSU Information Security Roles, Responsibilities, and Definitions

Information Technology Strategic Advisory Committee (ITSAC)

ITSAC is the senior university information technology committee charged with advising and providing recommendations on information technology issues to the President's Cabinet. ITSAC ensures that:

- The University makes the best possible decisions in advancing the acquisition, deployment, and use of technology in support of the goals outlined in the IT strategic plan; and
- Planning, pursuing new directions, institutional actions, and changes are implemented and integrated in a coordinated, collaborative, and transparent fashion.

See the ITSAC website for further information:

its.wsu.edu/it-strategic-advisory-committee-itsac/

Information System Owner

The information system owner is an organizational workforce member responsible for the procurement, development, integration, modification, operation, maintenance, retirement, and disposal of an information system. Responsibilities of the information system owner include:

- Addressing and satisfying the mission, business, and operational requirements of the institution or a specific business unit;
- Determine acceptable levels of risk for the organization
- Ensuring compliance with applicable information security and privacy requirements;
- Obtaining approvals for required security authorizations; and
- Maintaining required information system security, privacy, risk and compliance documentation.

DEFINITIONS

The following definitions apply to the University's Information Security Policy (EP37) and the University Data Policies (EP8):

Assurance

Assurance is defined as the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy.

Auditable Events

Auditable events are those information system security-relevant events which, when collected, analyzed, and correlated, can identify inappropriate, unusual, or suspicious activities and support after-the-fact investigations of security incidents.

WSU Information Security Roles, Responsibilities, and Definitions

Confidential Information

Confidential information is defined as information that is specifically protected by law, contracts, third-party agreements, or for other University business reasons as established by information owners.

Information in this category is to include:

- Personal information,
- Employee personnel records,
- Financial information,
- Donor information,
- Intellectual property,
- Attorney/client privileged information,
- Information regarding critical infrastructure of physical structures and assets,
- Security infrastructure of information technology systems,
- Passwords,
- Cryptographic private or shared keys,
- Cryptographic secrets,
- Authentication secrets or hashes, and
- Institutional strategies and methods that may be considered to provide a competitive advantage.

Criticality

Criticality is defined as a measure of the importance of the data to the University's mission and business operations. Data considered confidential may not necessarily be considered critical. Determining the criticality of a particular information system or data set must take into consideration the following:

- What is the impact to the University if the data is not recovered?
- How long will the data recovery process take?
- What is the effect of the loss of the data set during the recovery time, to include potential risks to the University (e.g., information security and privacy, strategic, financial, legal, regulatory, reputational, and operational)?

See also *BPPM* 90.15 regarding essential records protection.

WSU Information Security Roles, Responsibilities, and Definitions

Factor of Authentication

The term "factor of authentication" refers to an authenticator that conforms to one of the following types:

- Something you know – e.g. a password, passphrase, or PIN.
- Something you have – e.g. a physical object like a key, cell-phone, smart card, or other "hard token."
- Something you are – biometrics, e.g. a fingerprint, facial scan, or voice print.

Health Care Information

Health care information is defined as any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid (DNA) and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information.

See *RCW* 70.02.010.

Information Assurance

Information assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

Information Availability

Information availability is defined as the practice of ensuring timely and reliable access to and use of information.

Information Integrity

Information integrity is defined as the practice of ensuring information has not been improperly modified or destroyed and includes ensuring information nonrepudiation and authenticity.

Information Privacy

Information privacy is the practice of ensuring freedom from intrusion into the private life or affairs of individuals when that intrusion results from undue or illegal gathering and use of data about that individual.

Information Security

Information security is defined as the ability to ensure the confidentiality, integrity, and availability of institutional data held by WSU, regardless of its source or storage location.

Information System Users

Information system users are defined as individuals, or system processes acting on behalf of individuals, that are authorized to access a system.

WSU Information Security Roles, Responsibilities, and Definitions

Institutional Data

Institutional data are items of information, which are collected, used, and maintained by WSU for strategic and operational functions, to include administrative data and other data maintained and safeguarded for institutional purposes.

This data may be held across the WSU system by central administrative offices, colleges, departments, and/or workforce members (e.g., administrative staff, temporary and part-time employees, student employees, contractors, volunteers, third parties, and other authorized affiliates).

The University data policies apply to all institutional data, to include data held for the purposes of administration, research, scholarship, education, outreach, and engagement. (See EP8 and EP37.)

Institutional Information Systems and Services

Institutional systems and services are defined as the infrastructure, processes, procedures, and capabilities that allow the University devices to manage, collect, store, transmit, process, and share information in pursuit of its mission and business objectives.

Internal Information

Internal information is defined as information that is:

- Is not considered public;
- Is intended for internal WSU business purposes only; and
- Is considered operational in nature.

Examples of internal information may include information concerning various University business transactions and operations.

Least Privilege

The term "least priviledge" is defined as the principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Mobile Device

A mobile device is any hand-portable device capable of text, voice, e-mail, instant messaging (IM), photographic messaging, or other types of data communication. Desktop and laptop computers are not considered mobile devices.

Mobile Device Management (MDM)

Mobile device management (MDM) is software that allows agency support staff to manage a "sandbox" or container on a mobile device where state data and applications can be added, deleted, or monitored. Additional functions may include issuance, inventory tracking, and policy enforcement on the device.

WSU Information Security Roles, Responsibilities, and Definitions

NIST

The acronym "NIST" stands for National Institute of Standards and Technology.

Nonrepudiation

Nonrepudiation is defined as protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Personal Information

Personal information is an individual's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number; or the last four digits of the social security number;
- Driver's license number or Washington identification card number;
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;
- Full date of birth;
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- Student, military, or passport identification number;
- Health insurance policy number or health insurance identification number;
- Any information about a consumer's medical history, mental or physical condition, or a health care professional's medical diagnosis or treatment of the consumer; or
- Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patters or characteristics that may identify a specific individual.

The term "personal information" includes any of the above-listed data elements, alone or in combination, without the consumer's first name or first initial and last name, if encryption has not rendered the data elements unusable and if the data elements would enable a person to commit identity theft against a consumer.

WSU Information Security Roles, Responsibilities, and Definitions

Personal Information (cont.)

Personal information also includes username and email address in combination with a password or security questions and answers that would permit access to an online account.

See *RCW* 42.56.590.

Personally Identifiable Information (PII)

The term "personally identifiable information" includes, but is not limited to:

- A student's name;
- The name of the student's parent or other family members;
- The address of the student or student's family;
- A personal identifier, such as the student's social security number, student number, or biometric record;
- Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

See 34 *CFR* 99.3.

Plan of Action and Milestones (POAM)

A "plan of action and milestones (POAM)" is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Privileged Functions and Commands

Functions and commands that can only be executed by a person or process that has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer).

Protected Health Information (PHI)

Protected health information (PHI) is defined as any information, including demographic information collected from an individual, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

WSU Information Security Roles, Responsibilities, and Definitions

PHI (cont.)

- Relates to the:
  - The past, present, or future physical or mental health or condition of an individual;
  - The provision of health care to an individual;
  - The past, present, or future payment for the provision of health care to an individual; and:
    - Identifies the individual; or
    - For which there is a reasonable basis to believe that the information can be used to identify the individual.

See HIPAA Act of 1996.

Public Information

Public information is defined as information that is currently released or approved to be released to the public without restriction by the appropriate information owner or University administrator.

Examples of public information are:

- Employee directory information;
- Public University outreach and research publications;
- Press releases; and
- Information on the public WSU website.

Public Record

A public record includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

NOTE: Writing as used above means any form of communication or representation, including but not limited to letters, papers, maps, other communication on paper, as well as communication on e-mail, tape, film, video, magnetic or punched card, disk, sound recording, and computer data.

See *RCW* 42.56.010(3) and *BPPM* 90.05.

Regulated Information

Regulated information is defined as information that is specifically protected by federal, state, or industry laws, regulations, or standards for which strict protection, use, and handling requirements are dictated.

As an institution of higher education, WSU collects, stores, and processes a vast quantity of very sensitive data in conducting its day-to-day business operations and is therefore subject to the various information security and privacy laws that regulate the access, use, and handling of that information. The list below

WSU Information Security Roles, Responsibilities, and Definitions

Regulated Information (cont.)

includes, but is not limited to, specific laws and regulations that are included in this classification.

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Washington's Uniform Health Care Information Act (*RCW* 70.02)
- Payment Card Industry Data Security Standard (PCI DSS)
- European Union General Data Protection Regulation (GDPR)
- Protected Personal Information (*RCW* 19.255.010; *RCW* 42.56.590)
- Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
- Regulations Governing the Protection of Research Data (e.g., Federal Information Security Management Act (FISMA), Controlled Unclassified Information (CUI), Washington State Uniform Trade Secrets Act (*RCW* 19.108))
- National Security Information
- International Traffic in Arms Regulations (ITAR) (22 CFR 120-130)
- Export Administration Regulations (15 CFR 730-774)

Risk Management

Risk management is the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system, and includes:

- Conduct of a risk assessment;
- Implementation of a risk mitigation strategy; and
- Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Risk Assessment

Risk assessment is the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls

WSU Information Security Roles, Responsibilities, and Definitions

Risk Assessment (cont.)

that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

Rogue Device

An unauthorized client or access point on the WSU network, or an unauthorized access point seeking to impersonate the official WSU network.

Security Authorization

Security authorization is the official management decision given by a senior University official to:

- Authorize the operation of a system or the common controls inherited by designated organizations systems; and
- Explicitly accept the risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security and privacy controls.

The term "security authorization" is also known as "authorization to operate."

Separation of Duties

Separation of duties is a security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud.

Workforce Members

Workforce members are employees, volunteers, trainees, contractors, and affiliates with access to WSU information systems and institutional data.

MAINTENANCE

The Office of the CIO is to review this section (*BPPM* 87.01) and related policies EP37 and EP8 every three years or on an as-needed basis due to changes to technology environments, business operations, legal, or regulatory requirements.