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.


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 WSU system business units, workforce members, and WSU system 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 WSU System Data Policies (EP8).

Authorizing Official (AO)
An authorizing official (AO) is an executive head of a major WSU system 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 WSU official who is accountable for and is authorized to establish, maintain, and enforce a WSU system 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.
WSU Information Security Roles, Responsibilities, and Definitions

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.

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 WSU 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 WSU 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 WSU system 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.
WSU Information Security Roles, Responsibilities, and Definitions

**Information Owner (cont.)**
- Is 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.
- Has a duty to include appropriate stakeholders in evaluating risk and managing data (e.g., CIO, CISO, Chief Compliance and Risk Officer (CCRO)).
- May delegate these administrative duties to one or more WSU system 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.

**Information Technology Strategic Advisory Committee (ITSAC)**

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

- The WSU system 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.

**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;
- Determining acceptable levels of risk for the organization;
WSU Information Security Roles, Responsibilities, and Definitions

**Information System Owner**

- 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 WSU System 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.

**Business Associate**

A business associate is an individual, organization, or agency that provides services to a HIPAA-covered entity which requires them to have access to, store, use, or transmit protected health information.

**Confidential Information**

Confidential information is defined as information that is:

- Not covered under the definition of [regulated information](#);
- Specifically protected by law, contracts, third-party agreements; or
- For other WSU business purposes as established by information owners.

Information in this category is to include:

- Information about individuals that may be considered sensitive that is not defined as *personal information* in RCW 19.255.010 and RCW 42.56.590;
- Information about public employees as defined by RCW 42.56.250;
WSU Information Security Roles, Responsibilities, and Definitions

Confidential Info. (cont.)
- Lists of individuals for commercial purposes as defined by RCW 42.56.070(9);
- Financial information;
- Donor information;
- Intellectual property;
- Attorney/client privileged information;
- Information regarding critical infrastructure of WSU system physical structures and assets;
- Security infrastructure of information technology systems, networks, and services;
- 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.

Controlled Unclassified Information (CUI)
Unclassified information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under federal Executive Order 13526, Classified National Security Information, December 29, 2009.

For further information regarding WSU CUI, see the Office of Research DoD Proposals to Require Cybersecurity Certification website.

Covered Entity
Covered entities are defined in the HIPAA rules as:
- Health plans;
- Health care clearinghouses; and
WSU Information Security Roles, Responsibilities, and Definitions

Covered Entity (cont.)
- Health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards. (See 45 CFR 160.103).

Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit transaction information directly or through an intermediary to a health plan are covered entities.

Covered entities may be institutions, organizations, or persons.

Criticality
Criticality is defined as a measure of the importance of the data to the WSU system'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 WSU system (e.g., information security and privacy, strategic, financial, legal, regulatory, reputational, and operational)?

See also BPPM 90.15 regarding essential records protection.

Data Breach
A data breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses personally identifiable information; or
- An authorized user accesses personally identifiable information for another than authorized purpose.

Good faith acquisition of confidential or regulated information by an employee or agent of WSU for the purposes of conducting appropriate WSU business or operations is not a breach of the
WSU Information Security Roles, Responsibilities, and Definitions

Data Breach (cont.)

security of the system when the information is not used or subject to further unauthorized disclosure.

Export Administration Regulations (EAR)

The Export Administration Regulations (EAR) are a set of regulations found at 15 CFR 730 et seq. The EAR are administered by the Bureau of Industry and Security, which is part of the U.S. Department of Commerce.

In general, the EAR governs items considered to be of dual use. A dual use item is one that has civil applications as well as military. The EAR oversees all exports, reexports, and deemed exports that are considered duel use.

The EAR applies to physical things (sometimes referred to as commodities) as well as technology and software.

For further information on EAR at WSU, see the following websites:

- Office of Research Support and Operations (ORSO) Export Control Regulations
- Office of Research Assurances (ORA) Export Control Regulations

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, cellular telephone, 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.
WSU Information Security Roles, Responsibilities, and Definitions

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Research Subject Information</td>
<td>Information collected, stored, processed, or shared while conducting research activities that involve human subjects. For further information regarding human research subject information and the WSU Human Research Protection Program, see BPPM 45.50 and the Institutional Review Board website.</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>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.</td>
</tr>
<tr>
<td>Information Availability</td>
<td>Information availability is defined as the practice of ensuring timely and reliable access to and use of information.</td>
</tr>
<tr>
<td>Information Integrity</td>
<td>Information integrity is defined as the practice of ensuring information has not been improperly modified or destroyed and includes ensuring information nonrepudiation and authenticity.</td>
</tr>
<tr>
<td>Information Privacy</td>
<td>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.</td>
</tr>
<tr>
<td>Information Security</td>
<td>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.</td>
</tr>
<tr>
<td>Information Security Incident</td>
<td>An information security incident is defined as an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of WSU system information systems, services, devices, and data. (See also BPPM 87.55.)</td>
</tr>
<tr>
<td>Information System Users</td>
<td>Information system users are defined as individuals, or system processes acting on behalf of individuals, that are authorized to access a system.</td>
</tr>
<tr>
<td>Institutional Data</td>
<td>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.</td>
</tr>
</tbody>
</table>
WSU Information Security Roles, Responsibilities, and Definitions

Institutional Data (cont.)
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 WSU system 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 WSU devices to manage, collect, store, transmit, process, and share information in pursuit of its mission and business objectives.

International Traffic in Arms Regulations (ITAR)
The United States regulation overseen by the U.S. Department of State that controls the manufacture, sale, and distribution of defense and space-related articles and services as defined in the United States Munitions List (USML).

For more information regarding ITAR at WSU, see the following websites:

• Office of Research Support and Operations (ORSO) Export Control Regulations

• Office of Research Assurances (ORA) Export Control Regulations

Least Privilege
The term least privilege 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. (See BPPM 87.10 and 87.11 for description of applicable types of 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 institutional data and applications can be added, deleted, or monitored. Additional functions may include
WSU Information Security Roles, Responsibilities, and Definitions

MDM (cont.)

issuance, inventory tracking, and policy enforcement on the device. (See also BPPM 87.10 and 87.11.)

National Security Information

Information that has been determined pursuant to federal Executive Order 12356 of December 30, 2009, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

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 a term defined by the state of Washington in RCW 42.56.590 as 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 or more 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;
WSU Information Security Roles, Responsibilities, and Definitions

Personal Information (cont.)

- 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 patterns 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.

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 19.255.010 and RCW 42.56.590.

Personally Identifiable Information (PII)

The term personally identifiable information (PII), as defined under FERPA, refers to identifiable information that is maintained in education records. PII 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
WSU Information Security Roles, Responsibilities, and Definitions

PII (cont.)
- 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 for a complete definition of PII specific to education records and for examples of data elements that are defined as PII.

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
- 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.

WSU Information Security Roles, Responsibilities, and Definitions

Public Information
Public information is defined as information that can be or is currently released to the public without restriction.

Examples of public information are:

- Employee directory information;
- Widely distributed materials;
- Public WSU 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 confidential information that is specifically protected from disclosure by law and for which there are strict information handling requirements that are dictated by statutes, regulations, or agreements.

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 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)
WSU Information Security Roles, Responsibilities, and Definitions

Regulated Info. (cont.)

- 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)
- Children's Online Privacy Protection Act (COPPA)
- China's Personal Information Protect Law
- Payment Card Industry Data Security Standard (PCI DSS)
- European Union General Data Protection Regulation (GDPR)
- Personal Information as defined by RCW 19.255.010 and 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 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 that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
WSU Information Security Roles, Responsibilities, and Definitions

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.

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 WSU system 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.

WSU Internal Information
WSU internal information is defined as information that is for internal WSU business purposes only and may not be specifically protected from disclosure by law.
WSU Information Security Roles, Responsibilities, and Definitions

Internal Information (cont.)
Examples of WSU internal information may include information concerning various WSU system business transactions and operations.

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.