Information Security Planning

OVERVIEW

Washington State University is accountable for protecting the confidentiality, integrity, availability, and privacy of institutional systems and information.

This policy (*BPPM* 87.15) describes the information security planning requirements and processes for the effective implementation of information security controls to meet the appropriate information system security and privacy objectives. The policy establishes:

- Information system and service roles and responsibilities; and
- Management commitment for information security planning purposes during:
    - System design,
    - Implementation; and
    - Placing an information system into service.

See *BPPM* 87.01 for definitions related to this section. See also *BPPM* 87.20: Security Assessment and Authorization and the WSU Information Security Control Objectives.

Purpose

This BPPM governs information technology (IT) systems/services at Washington State University (WSU). It defines:

- System/service ownership and management responsibilities;
- Development and documentation requirement; and
- IT system/service authorization.

Scope

This policy (*BPPM* 87.15) applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

POLICY

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

IMPORTANT: Information owners are to develop procedures to implement this policy (*BPPM* 87.15) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Information System/ Service Owner

Every institutional information system/service must have an identified information system/service owner to ensure that institutional information systems and services meet the appropriate information security and privacy requirements.

Information Security Planning

System Security Plan

Information owners designate the information system/service owners for information systems and services under their care. System security plans are to be developed to facilitate the implementation of this policy and address:

- Appropriate information security and privacy objectives and risks;
- Required information system security and privacy requirements; and
- Related controls.

System security plans are to be disseminated to the appropriate business unit personnel according to their roles.

The information system/service owner must prepare a system Security Plan (SSP) for all information systems/services under their care. The SSP describes the:

- IT system/service;
- Information security and privacy requirements; and
- Security and privacy controls, processes, or procedures to be in place for meeting those requirements.

A complete SSP helps to support the decision-making process for the authorizing official to approve the operation of an information system or service.

Approval

SSPs are reviewed and approved by a business unit authorizing official prior to system implementation.

Updates

SSPs are updated by the information system/service owner, or their appropriate designee, at least annually or when required by information system/environment changes.

Protection

SSPs are protected from unauthorized disclosure and modification.

Specific SSP Criteria

The SSP must adhere to the following criteria.

Scope and Objectives

Define the scope and strategic objectives of the IT system/service.

Operational Context

Describe the operational context of the information system in terms of missions and business processes.

Information Security Planning

Safeguards

Provide for and document the appropriate safeguards for the information system including supporting rationale, according to the:

- Mission criticality of the system;
- Classification of data the information the system will be handling;
- Applicable legal, regulatory, and contractual requirements.

Operational Environment

Describe the operational environment for the information system as follows:

- The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization's control), as applicable;
- Describe the authorization boundary of the system and any relationships/connectivity to other information systems;
- The operational environment must be consistent with institutional information technology and security architectures.

Security Requirements

Describe the security controls in place, or the plan for meeting those requirements, including a rationale for the decisions and a schedule for implementing planned controls.

User Responsibilities

Describe information system user responsibilities and expected behavior regarding information and information system usage.

Risk Management

Describe how existing or planned security controls provide adequate mitigation of risks to which the IT system is subject.

Information Security Controls

Information system owners are to ensure the appropriate administrative, technical, and physical security and privacy controls are implemented in the IT systems/services environments within their area of responsibility and documented in the system security plan (SSP).

The WSU set of common information security control objectives are listed in WSU Information Security Control Objectives on the IT website.

Information Security Planning

Information Security Architecture

The information security architecture of the information system/service must be developed and documented in the SSP:

- Provide an overview of the information security requirements;
- Describe the overall approach taken in regard to appropriately protecting the institutional information systems and data;
- Describe the information security architecture of the information system and how it is integrated into Institutional information security architectures; and
- Describe any information security assumptions and any dependencies on external systems/services, relative to the particular information system being developed and implemented.

ENFORCEMENT

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, *WAC* 504-26).

Exceptions

Exceptions to this policy are managed and maintained by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CSIO).

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.