Configuration Management

OVERVIEW

Configuration management provides an important function for establishing and maintaining secure information system configurations and important support for managing risks in information systems.

See *BPPM* 87.01 for definitions related to this section.

Purpose

The purpose of this policy (*BPPM* 87.30) is to:

- Provide objectives for managing the configuration of the WSU information systems and associated components for secure processing, storing, and transmitting of information in the information environment;
- Describe roles and responsibilities, general practices and activities, and artifacts necessary to guide the configuration management process for key information systems and capabilities; and
- Control the maintenance of Information Technology (IT) systems, using best practice approaches to tracking all configuration change requests.

Scope

This policy 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 must develop procedures to implement this policy (*BPPM* 87.30) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Configuration Management Process

Information system owners must maintain a configuration management process that addresses:

- Scope;
- Roles;
- Responsibilities;
- Management commitment; and
- Coordination among organizational entities.

Configuration Management

Configuration Mgmt. Process (cont.)	Information system owners must designate appropriate resources to manage development, documentation, and dissemination of configuration management procedures and processes. Information system owners are to review and update these procedures and processes at least annually or when required by a significant change in system components or configuration.
Configuration Management Plan	The configuration management plan must include procedures to facilitate the implementation of the process and the associated configuration management controls, including: • Roles and responsibilities; and • The method to identify configuration items throughout the system development life cycle. Information system owners are to protect the configuration management plan from unauthorized disclosure and modification.
Current Baseline Configuration	Information system owners are to develop, document, and maintain a current baseline configuration for each information system in their area of responsibility that is under configuration control.
Security Controls	The required information security controls are to be implemented at the time of system deployment and throughout the life cycle of the system. This includes physical and logical access restrictions when making changes to the system(s).
Configuration Control Changes	Information system changes that are under configuration control are to be defined in the configuration management process. Information system owners must: • Coordinate configuration change control activities with oversight from a business unit (area, college, or department) change control board or committee that convenes every 30 days as a minimum. • Document and associate configuration change decisions with the information system. • Retain records of configuration-controlled changes to the information system from the last major upgrade/version change or significant modification of the security model of the service/solution.

Configuration Management

Configuration Setting Changes

All information system configuration changes that affect the security posture and/or functionality of the system are to be monitored and controlled. Information system owners must:

- Analyze information system changes to determine potential security impacts prior to change implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- Configure information systems to operate at the most restrictive mode consistent with operational requirements.
- Identify, document, and approve any deviations from established configuration settings for information system components.

Hardware and Software Inventory

Information system owners must maintain an inventory of information system hardware and software components that are under configuration management control. The inventory must accurately reflect the current information system state, including all components within the authorization boundary of the information system.

- The inventory must be at the level of granularity to allow for tracking and reporting.
- The inventory is to be reviewed and updated every six months, at a minimum.

Software Installation

Information system owners are to establish policies and processes to govern the installation of software by administrators and users.

Use Tracking and Licenses

The use of software must be tracked and associated documentation protected by licenses to control copying and distribution.

Enforcement and Monitoring

Software installation enforcement and monitoring policies and processes:

- Software installation policies are to be enforced using technological methods and monitored for compliance annually.
- Information system owners or administrators must develop procedures to enforce user software installation policies and procedures.

Configuration Management

Enforcement and Monitoring (cont.)

- Information system owners or administrators must monitor user software installation policy compliance no less than annually.

ENFORCEMENT

The Office of the 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 must be 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.