Security Assessment and Authorization

OVERVIEW

Security authorization (SA) is the official management decision given by executive University officials or their designees to:

- Authorize operation of an institutional information system; and
- Explicitly accept the risk to University operations and assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security controls.

Security authorization:

- Involves the evaluation of security processes and controls of an information system;
- Addresses software and hardware security safeguards, to include the administrative, technical, and physical security measures; and
- Establishes the extent to which a particular design (or architecture), configuration, and implementation meets a specified set of security requirements throughout the life cycle of the information system.

See *BPPM* 87.01 for definitions related to this section. See also the Guidelines for Developing a Security Assessment Plan on the IT website.

Purpose

The security authorization process includes conducting the following activities:

- Information and system classification,
- Information security and privacy control selection, implementation, and assessment,
- Information system authorization, and
- Security and privacy control monitoring.

The SA process helps ensure that managing information system-related security risks is consistent with the University's mission/business objectives and overall risk strategy established by Enterprise Risk Management Services and the Office of the Chief Information Officer (CIO). Integrating information security and privacy safeguards into the University's enterprise architecture process supports consistent, well-informed security authorization decisions throughout the life-cycle of the information system.

Security Assessment and Authorization

Purpose (cont.)

The purpose of this policy (*BPPM* 87.20) is to provide high level requirements and practical guidance for conducting a security assessment within the institutional information technology (IT) environment. The Office of the CIO develops, documents, and disseminates this policy to University area technology officers and administrators.

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

Accountability

Information owners are accountable for:

- Operation of information systems within their areas of authority;
- Authorization processes used to officially declare that an information system is authorized to operate within the institutional IT operating environment; and
- Development of appropriate procedures for the implementation of this policy.

Developing Procedures

IMPORTANT: Information owners must develop procedures to implement this policy (*BPPM* 87.20) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Security assessment and authorization procedures are to be:

- Distributed to appropriate University business unit personnel according to their roles; and
- Updated by the information system owner, annually or when required by information system/environment changes.

Conducting Assessments

Information owners are to utilize centralized resources and processes for conducting information security and privacy assessments where operationally feasible to do so.

Security Assessment and Authorization

Security Assessment Plan

Information system owners must prepare a security assessment plan for information systems and services under their care that describes the scope of the assessment. The plan is to include the:

- Information security and privacy controls under assessment;
- Assessment procedures to be used to determine security control effectiveness;
- Assessment environment,
- Assessment team;
- Assessment roles and responsibilities; and
- Assessment of the information security controls of the information system and its environment of operation, which is to be conducted at least annually. This assessment must determine the extent to which the security controls are:
    - Implemented correctly;
    - Operating as intended; and
    - Producing the desired outcome with respect to meeting established security requirements.

Security Assessment Report

The assessment team must produce and provide a security assessment report documenting the results of the assessment to the:

- Information owner;
- Information system owner; and
- Responsible business unit data custodian.

Data Sharing

The appropriate information owners or their designees authorize any interconnectivity and data sharing between institutional information systems within the University and organizations that are external to the University.

Data Sharing Agreements

Data sharing agreements are to include, at a minimum, the information security and privacy requirements and the nature of the information to be shared. The appropriate information owners or their designees are to periodically review the data sharing agreements.

Security Authorizations

Information owners or their designees are assigned as authorizing officials for the information systems/services within their areas of responsibility. Authorizing officials are to approve information systems and services for processing before information systems are placed into service.

Security Assessment and Authorization

Reauthorizations

Security authorizations are updated annually. Security reauthorizations are to be based on:

- Employment of continuous monitoring processes;
- Security assessment reports; and
- Plan of action and milestones.

Continuous Monitoring

Institutional business units are to develop a continuous monitoring strategy and implement a continuous monitoring program that includes the:

- Information system metrics to be monitored;
- Frequency that the system to be monitored;
- Frequency of security assessments supporting such monitoring;
- Ongoing security control assessments;
- Ongoing security status monitoring;
- Correlation and analysis of security-related information generated by assessments and monitoring;
- Response actions to address results of the analysis of security-related information; and
- Reporting requirements on the status of institutional information systems to the responsible information owners, other appropriate busines unit personnel according to their roles, and the CISO.

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 are managed and maintained by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CISO).

Security Assessment and Authorization

Exceptions (cont.) 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.