Information Security Risk Assessment

OVERVIEW

An information security risk assessment is used to identify potential threats to information systems and data and analyze the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction. if a threat were to be realized.

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

Purpose

This policy (*BPPM* 87.25) has been developed to assist risk-based decision-making in support of WSU's mission and business objectives. This policy provides the framework to incorporate consistent and effective risk assessment into the strategic and operational planning processes in order to manage the impact of potential harm.

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* 87.25) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Responsibility

The Chief Information Security Officer (CISO) is responsible for WSU's Information Security program, including information security and privacy risk management oversight. The CISO provides an appropriate methodology to help identify, evaluate, and appropriately respond to information security and privacy risks in support of the University's mission and business objectives.

Security Categorization

Information systems and the information collected, processed, stored, and transmitted by the systems are to be categorized in accordance with *Executive Policy Manual* EP8: University Data Policies.

- Security categorization results, including supporting rationale, are to be documented in the system security plan for the information system. (See *BPPM* 87.15.)

- The information owner, their designee, or the appropriate data custodian review and approve business unit information categorizations.

Information Security Risk Assessment

Conducting Assessment

An assessment of risk must be conducted that includes the likelihood and magnitude of harm possible from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it collects, processes, stores, or transmits.

The risk assessment is to be conducted:

- Annually;
- Whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities); or
- Whenever other conditions arise that may impact the security posture of the system.

Confidential or Regulated Data Vulnerability Scans

Business units are responsible for scanning for vulnerabilities all applicable information systems and services that collect, store, process, transmit, and/or use institutional confidential or regulated data. Vulnerability scans are to be conducted every 30 days or when significant new vulnerabilities potentially affecting the system are identified and reported.

See also Risk Assessment Report.

Reports and Assessment Results

Business units must analyze vulnerability scan reports and security control assessment results to assess impact. Legitimate vulnerabilities are to be remediated in accordance with University policies and business unit procedures.

Business units are to share vulnerability scanning and security control assessment results with the:

- Information system or service owner;
- Individuals having information security roles and responsibilities for the system; and
- Organizational personnel responsible for helping to remediate similar vulnerabilities in other institutional information systems.

Vulnerability scanning tools and techniques should support interoperability among tools where operationally feasible.

Information Security Risk Assessment

Network and System Vulnerability Scans

Information system or service owners are to coordinate with Information Security Services to conduct network and system vulnerability scans of their information systems or services. (See also Risk Assessment Report below.)

Risk Assessment Report

Risk assessment results, to include vulnerability scan results, are to be documented in a risk assessment report.

Risk assessment results are to be disseminated to the:

- Information owner or their designee;
- Appropriate data custodian;
- Information system or service owner; and
- CISO or the CISO's designee.

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 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.