System and Information Integrity

OVERVIEW

The discipline of information systems security relies on the practice of ensuring and maintaining the confidentiality, integrity, and availability of information systems and the data transmitted, processed, and/or stored on those systems. Integrity is defined as guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. It is the assertion that data can only be accessed or modified by authorized entities.

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

Purpose

System and information integrity provide assurance that the information being accessed has not been tampered with or damaged by an error in the information system. Examples of system and information integrity requirements include:

- Flaw remediation;
- Malicious code protection;
- Information system monitoring;
- Security alerts;
- Information input validation;
- Error-handling; and
- Memory protection.

Scope

This policy (*BPPM* 87.35) 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* 87.40) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Before Installation

Before installation of information systems, institutional business units must:

- Identify, report, and correct information system flaws; and

- Test software updates on nonproduction systems for potential side effects on University information assets.

System and Information Integrity

Software and Firmware Updates

After installation, institutional business units must install security-relevant software and firmware updates within an appropriate amount of time, in accordance with University policies and business unit procedures.

Flaw Remediation

Automated processes are to be used continuously to identify the state of information systems regarding flaw remediation.

Malicious Code Protection Mechanisms

Malicious code protection mechanisms must be employed at information system entry and exit points as well as system endpoints to detect and eradicate malicious code. The malicious code protection mechanisms are to be automatically updated whenever new releases are available, in accordance with University policies and business unit procedures.

Configuration

Malicious code protection mechanisms are to be configured to perform periodic scans of the information systems and take automated actions against any malicious code that is found. Information systems are to be scanned on a regular basis for malicious code and in real-time on system endpoints and information system exit points, as files are downloaded, opened, or executed.

Malicious Code Detection

On detection of malicious code, the malicious code protection mechanisms must block and/or quarantine malicious code and send alerts to the Washington State University (WSU) Security Operations Center (SOC).

Monitoring

In accordance with the University's established logging and monitoring objectives, WSU policies, and applicable laws, regulations, and standards, institutional business owners must ensure that information systems are monitored to detect:

- Attacks;
- Indicators of potential attacks; and
- Unauthorized use.

Regular Monitoring

Information systems as well as information system boundaries (i.e., perimeters) are to be monitored continuously to provide near real-time analysis of alerts and/or notifications generated by institutional information systems.

Heightened Risk Monitoring

The level of information system monitoring is to be heightened when there is an indication of increased risk to University operations and assets, individuals, and/or other organizations.

System and Information Integrity

Alerts

Malicious Code

When indications of compromise are received from malicious code protection mechanisms, automated alerts are generated and sent to the WSU SOC.

External Security Alerts, Advisories, and Directives

Business units are to receive information system security alerts, advisories, and directives on an ongoing basis from:

- United States Computer Emergency Readiness Team (US-CERT);
- Washington State Office of the Chief Information Officer (OCIO);
- Other organizations, as warranted.

Internal Security Alerts, Advisories, and Directives

Business units must ensure that internal security alerts, advisories, and directives are generated as deemed necessary and disseminated to institutional area technology officers (ATOs), information system owners, and other appropriate business unit personnel according to their roles.

Implementation

Security alerts, advisories, and directives must be implemented within established time frames defined in University polices and business unit procedures.

List of Authorized Information Systems

Business units must maintain a list of authorized business information systems and software and protect the list from the loss of integrity.

Integrity Checks

Integrity checks of the authorized business systems and software are to be performed during system startup, restart, and shutdown.

Unauthorized Change Detection

The detection of unauthorized changes to authorized business systems and software must be integrated into University business unit incident response processes.

Spam Protection

Centrally managed spam protection mechanisms must be employed at information system entry and exit points to detect and take action on unsolicited messages.

Automatic Updates

Information systems are to be automatically updated when new releases become available, in accordance with University policies and business unit change management processes.

System and Information Integrity

Input Validity Checks

Where operationally feasible, institutional information systems are to check the validity of system inputs to help ensure accurate and correct inputs and prevent cyberattacks, such as cross-site scripting and a variety of injection attacks. System inputs may include, but are not limited to, character set, length, numerical range, and acceptable values.

Error Messages

University information system developers must ensure error messages generated from the information system provide the information necessary for corrective actions without revealing information that could be exploited by adversaries.

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.