System and Information Integrity Standard

Introduction

Access to system information owned or operated by the State of Oklahoma is provided to employees and contractors for use to support the mission of the state. As such, system and information integrity must be maintained to ensure the accessed information has not been tampered with or damaged by an error in the information system. System and information integrity guards against improper information modification or destruction.

Purpose

This standard establishes OMES IS policy for managing risks from system flaws, vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective system and information integrity program. This standard helps the State of Oklahoma implement security best practices with regards to system configuration, security and error handling.

The scope of this policy is applicable to all information technology resources owned or operated by the State of Oklahoma. Any information not specifically identified as the property of other parties that is transmitted or stored on OMES IT resources (including email, messages and files) is the property of the State of Oklahoma. All users (State of Oklahoma agency employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

This standard is consistent with best practices associated with organizational information security management. This standard also establishes a system and information integrity capability throughout state agencies to help implement security best practices with regards to system configuration, security, and error handling.

Standard

The State of Oklahoma has chosen to adopt the system and information integrity principles established in NIST SP 800-53 System and Information Integrity, Control Family guidelines, as the official policy for this domain. The following subsections outline the system and information integrity standards required by the State of Oklahoma. Each State of Oklahoma agency is bound to this requirement and must develop or adhere to a program plan which demonstrates compliance.

- SI-1 system and information integrity procedure – All agencies must develop, adopt or adhere to a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- SI-2 flaw remediation – All agencies must:
    - Identify, report and correct information system flaws.
    - Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
    - Incorporate flaw remediation into the organizational configuration management process.
- SI-3 malicious code protection – All agencies must:

    - Employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., email, removable media and malicious websites) on the network to detect and eradicate malicious code.
    - Update malicious code protection mechanisms, including signature definitions, whenever new releases are available, in accordance with organizational configuration management requirements.
    - Configure malicious code protection mechanisms (e.g., real-time scans, periodic scans, malicious code detection) to protect state information systems and assets.
    - Address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of the information asset.
- SI-4 information system monitoring – All agencies must:
    - Monitor events on the information asset and detect information asset attacks.
    - Identify unauthorized use of the information assets.
    - Deploy monitoring devises (i) strategically within the information asset to collect organization-determined essential information, and (ii) at ad-hoc locations within the system to track specific types of transactions of interest to the organization.
    - Heighten the level of information asset monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information or other credible sources of information.
    - Obtain legal opinion with regards to information asset monitoring activities in accordance with applicable federal laws, directives, policies or regulations.
- SI-5 security alerts, advisories and directives – All agencies must:
    - Receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
    - Generate internal security alerts, advisories and directives to key system owners and stakeholders.
    - Implement security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.
- SI-6 security functionality verification – All agencies must verify the correct operation of security functions on an annual basis and notify the system administrator when anomalies are discovered to ensure timely corrective action.
- SI-7 software and information integrity – All agencies must detect unauthorized software changes within their information asset.
- SI-8 spam protection – All agencies must employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. In addition, state agencies must update spam protection mechanisms (including signature definitions) when new releases are available in accordance with OMES configuration management requirements.
- SI-9 information input restrictions – All agencies must restrict the capability to input information to the information asset to authorized personnel.
- SI-10 information input validation – All agencies must check the validity of information inputs for State of Oklahoma assets.
- SI-11 error handling – All agencies must have information assets that:
    - Identify potentially security-relevant error conditions.
    - Generate error messages that provide information necessary for corrective actions without revealing state sensitive information in error logs and administrative messages that could be exploited by adversaries.
    - Reveal error messages only to authorized personnel.

- SI-12 information output handling and retention – All agencies must handle and retain both information within and output from the information system in accordance with applicable state and federal laws, directives, policies, regulations, standards and operational requirements.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publications 800-53 Recommended Security Controls for Federal Information Systems Revision 3, Operational Controls, System and Information Integrity Control Family, August 2009.
- NIST Special Publications 800-100 Information Security Handbook: A guide for Manager, October 2006.
- NIST Special Publications 8000-40 Creating a Patch and Vulnerability Management Program, November 2005.
- NIST Special Publications 800-83 Guide to Malware Incident Prevention and Handling, November 2005.
- NIST Special Publications 800-61 Computer Security Incident Handling Guide, March 2008.
- NIST Special Publications 800-92 Guide to Computer Security Log Management, September 2006.
- NIST Special Publications 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.
- NIST Special Publications 800-45 Guidelines on Electronic Mail Security, February 2007.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/16/2022	**Review cycle:** Quarterly
Last revised: 12/16/2022	**Last reviewed date:** 12/16/2022
Approved by: Jerry Moore, Chief Information Officer	