Application Security Standard

Introduction

The State of Oklahoma must ensure the confidentiality, integrity, and accessibility of its information systems. By establishing minimum security standards, the state can better prevent or mitigate malicious actions by threat actors attempting to disrupt state operations or steal citizen data.

Purpose

This document establishes the minimum-security standards to which any software application in use on State of Oklahoma computers or systems must adhere and include the following:

- Data encryption.
- System and information integrity.
- Network protection.
- Application security logging.

The recommendations in this document are a starting point, however the controls and configurations described are not complete, nor are they intended to be. This standard is a baseline configuration that can be expanded to meet the needs of highly regulated or specific use-case systems.

Definitions

FIPS – Federal Information Processing Standards; a set of publicly announced standards developed by the National Institute of Standards and Technology.
SI – System and information integrity.
TLS – Transport Layer Security; an authentication and encryption protocol widely implemented in browsers and web servers.

Standard

Data encryption.

- Data must be encrypted using TLS 1.2 or newer to encrypt authentication and data in transit between computers or systems.
- Data must be encrypted while at rest utilizing FIPS 140-2/3 validated encryption modules or better.

System and information integrity.

The State of Oklahoma has chosen to adopt the system and information integrity principles established in NIST SP 800-53 Rev 5.1.1 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 with the following controls:

- 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 devices strategically within the information asset to collect organization-determined essential information and 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.

Network protection.

Any application utilizing the State of Oklahoma computer network to transmit or receive data must be compatible with and make use of the following network security controls:

- Network flow visibility tools.
- Intrusion Prevention/Detection Systems (IPS/IDS).
- Network Detection and Response (NDR).
- Attack Surface Management Tools (ASM).

Application security logging.

Any application or system used by the State of Oklahoma must maintain audit and/or file logs for a period of one year at minimum, or longer as required by federal or state laws or regulations. Information collected and stored may include, but is not limited to, user identification, date and time of the session, software used/accessed, files used/accessed, internet use and access, when requested and deemed necessary to ensure the confidentiality, integrity and accessibility of systems and associated data.

OMES reserves the right to view or scan any file or software stored on the computer or passing through the network and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as malware) or to audit the use of state resources.

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

- NIST SP 800-53 Rev 5.1.1.

- FIPS 140-2 Security Requirements.
- FIPS 140-3 Security Requirements.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 05/23/2025	**Review cycle:** Annual
Last revised: 05/23/2025	**Last reviewed:** 05/23/2025
Approved by: Dan Cronin, Chief Information Officer	