Least Functionality Standard

Introduction

The State of Oklahoma Office of Management and Enterprise Services has established a standard of least functionality in accordance with NIST SP 800-171.

The principle of least functionality provides that information systems are configured only to provide essential functionality and to restrict any non-essential functionality. This applies to ports, protocols, services and applications that are not integral to the operation of that information system.

Purpose

This document establishes and defines the OMES least functionality requirements for configuring information systems in order to lessen attack vectors and reduce risks to an acceptable level.

Standard

1. Information systems components should specifically prohibit or restrict non-essential functionality and provide only the required minimum functionality needed to perform its assigned business function.
2. Information systems components should be limited to a single function per device where feasible.
3. Access to OMES resources should be granted and managed based on user role and job functions and restricted to only those requiring access for their assigned job functions. This includes both logical and physical access.
4. Any functions, ports, protocols and services within information systems deemed unnecessary or insecure should be disabled to prevent unauthorized access.
5. Any applications deemed unnecessary for the functionality of the system should be uninstalled if practicable. If they cannot be uninstalled, they must be disabled or blocked from execution and/or communication.
6. The systems must be reviewed on a regular basis to ensure that least functionality is maintained.

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 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC.
- NIST SP 800-171A Rev. 3, Assessing Security Requirements for Controlled Unclassified Information | CSRC.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/13/2025	**Review cycle:** Annual
Last revised: 01/13/2025	**Last reviewed:** 01/13/2025
Approved by: Dan Cronin, Chief Information Officer	