OKLAHOMA
Office of Management
& Enterprise Services

Exchanges of Information and Software Standard

Introduction

Information can be vulnerable to unauthorized access, misuse or corruption physical transport, for instance when sending media via the postal service or via courier. As such, media being transported must be protected from unauthorized access, misuse or corruption.

Purpose

Exchanges of information and software between organizations should be controlled and compliant with any relevant legislation.

Standard

Exchanges of information and software should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit must be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should include:

- Responsibilities for controlling and notifying transmission, dispatch and receipt.
- Procedures for notifying sender, transmission, dispatch and receipt.
- Minimum technical standards for packaging and transmission.
- Courier identification standards.
- Responsibilities and liabilities in the event of loss of information.
- Information and software ownership and responsibilities for information protection, software copyright compliance and similar considerations.
- Technical standards for recording and reading information and software.
- Any special controls that may be required to protect sensitive items, such as cryptographic.

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

- Information Security Policy, Procedures and Guidelines.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 09/06/2024	**Review cycle:** Annual
Last revised: 09/06/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	