Confidential Technology Standard

Introduction

The State of Oklahoma maintains confidential and proprietary standards for information not generally available to employees or the public. These standards apply to, but are not limited to, those associated with life safety, cyber security and other critical business functions.

Confidential standards are held in strict confidence, unless there is a legitimate business need to provide to an agency or vendor as determined by the state CIO.

Purpose

This document identifies how confidential standards are classified by sensitivity and the process for requesting the review of these standards.

Standard

OMES IS uses Traffic Light Protocol to ensure sensitive information is shared with the correct audience. TLP employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s):

- TLP:RED – Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED with any parties outside of the specific exchange, meeting or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
- TLP:AMBER+STRICT – Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organization. Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
- TLP:AMBER – Sources may use TLP:AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
- TLP:GREEN – Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- TLP:CLEAR – Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP:CLEAR information may be distributed without restriction, subject to copyright controls.

Information in confidential standards is TLP:RED and is also privileged and confidential under the Oklahoma Open Records Act. 62 O.S., § 34.12(C). The Oklahoma Open Records Act provides that the chief information officer and OMES IS shall not be required to disclose, directly or indirectly, any information of a state agency which is declared to be confidential or privileged by state or federal statute or the disclosure of which is restricted by agreement with the United States or one of its agencies, nor disclose information technology system details that may permit the access to confidential information or any information affecting personal security, personal identity, or physical security of state assets. Additionally, 51 O.S., § 24A.28 provides that certain information technology information may be treated as confidential. The chief information officer

and the chief information security officer may restrict access pursuant to TLP. Unauthorized access is prohibited and subject to civil and criminal penalties.

Access to review confidential and proprietary standards may be granted at the sole discretion of the state CIO. To request review, individuals contact the office of the CIO with their specific review request and a compelling justification. Should the request be approved; an appointment is coordinated for an on-site review of the standard. No recordings of the discussion or pictures of the standard are permitted.

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.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/06/2021	**Review cycle:** Annual
Last revised: 07/27/2023	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	