Introduction
Oklahoma Cyber Command is responsible for protecting state users and their devices, networks, data and applications. Oklahoma Cyber Command’s top priority is safeguarding the state’s data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss. The OMES IS division supports Cyber Command’s vision to provide leadership in the development, delivery and maintenance of cybersecurity, information security risk management, enterprise fraud, physical security systems, compliance and privacy programs.

Purpose
This document defines the authority of and services provided by Oklahoma Cyber Command.

Standard
Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. §§ 34.11.1, including, but not limited to the following.

- **Defensive services:**
  - Endpoint management.
  - Virtual Desktop Infrastructure (VDI).
  - Endpoint Detection and Response (EDR).
  - Endpoint encryption.
  - Vulnerability management.
  - Secure Mail Gateway (SMG).
  - Secure Web Gateway (SWG).
  - Virtual Private Network (VPN).
  - Multi-Factor Authentication (MFA).
  - Privilege Access Management (PAM).

- **Compliance/Privacy services:**
  - Auditing.
  - Consultation with regulatory entities.
  - Project support.
  - Security Education and Awareness Training (SEAT).
  - Annual risk assessments.
  - Incident support.
  - Background clearances.
  - eDiscovery support.
  - Data Loss Prevention/Digital Rights Management (DLP/DRM).
  - Data classification.
  - Privacy impact assessments.

- **Offensive services:**
  - Access control.
  - Threat intelligence collection, analysis, exploitation and production.
  - Forensics.
  - Investigations.
  - Threat assessments.
  - Threat monitoring and analysis.
It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma Cyber Command.

Through the Oklahoma Information Sharing and Analysis Center (OK-ISAC), Oklahoma Cyber Command maintains relationships and facilitates information sharing between regulatory bodies, including federal partners, industry oversight bodies and state/local law enforcement agencies to monitor cyber trends and help reduce the risk of cyber threats.

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
- Oklahoma OMES Cyber Command.
- OMES Unified but not Consolidated.

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

<table>
<thead>
<tr>
<th>Effective date: 04/07/2022</th>
<th>Review cycle: Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last revised: 04/07/2022</td>
<td>Approved by: Jerry Moore, Chief Information Officer</td>
</tr>
</tbody>
</table>