STATE OF OKLAHOMA INFORMATION SECURITY POLICY, PROCEDURES AND GUIDELINES (PPG)

THIS PAGE LEFT BLANK

INTRODUCTION

This document is a compilation of the Information Security standards for the State of Oklahoma and provides an easy reference to the published security standards for the state.

These standards describe the minimum acceptable security posture for state agency information systems, and for vendor partners providing either on-premises or cloud-based information systems to the state.

Certain legacy systems might not be capable of meeting these standards, or proposed solutions might require either a full or partial exception to one or more of the standards. In general, as long as proposed changes or exceptions do not result in an overall reduction of security policy, they will be granted in a timely manner to ensure that ongoing work is not unduly delayed. In these instances, requests should be made to Oklahoma Cyber Command for any exceptions as needed.

All information security standards are reviewed at least annually and updated as needed. The following link leads to all current standards for the State of Oklahoma approved by the OMES Chief Information Officer in accordance with Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8.

Policy & Standards (oklahoma.gov).

OMES IS SECURITY STANDARDS

1. ACCESS CONTROL
   - Identity Management Standard.
   - Physical Access Control Standard.

2. AGENCY SECURITY
   - Non-unified agencies should follow the security standards listed on the OMES IS Policy & Standards website.

3. AWARENESS/TRAINING
   - Security Awareness Training Standard.

4. CENTRAL SECURITY PROGRAM
   - Security Services Standard

5. CONTROLS ON MALICIOUS SOFTWARE
   - Security Services Standard
   - Endpoint Protections and Connectivity Standard.

6. DISPOSAL OF MEDIA
   - Media Disposal Standard.

7. ELECTRIC COMMERCE SECURITY
   - Guidelines for the Evaluation of Electronic Data Interchange Products – NIST Special Publication 500-231.
   - Multifactor Authentication for E-Commerce - NIST SPECIAL PUBLICATION 1800-17.

8. EMAIL USAGE
   - Email Acceptable Use Standard.

9. EXCHANGES OF INFORMATION AND SOFTWARE
   - Exchanges of Information and Software Standard.
   - API Management Standard.
   - Batch File Transfer Standard.

10. THIRD PARTY RISK
- IT Contractor Requirement Standard.
- Third-Party Cybersecurity Management Standard.
- Offshore Data Storage Standard.

11. HOSTING AGENCY SECURITY
- Workstation Standard.
- Mobile Services Standard.
- Mobile Device Platform Standard.
- State Data Platform Standard.
- Data Storage Standard.
- Enterprise Reference Architecture Standard.

12. INCIDENT MANAGEMENT & SECURITY REPORTING PROCEDURE
- Incident Response Standard.

13. INFORMATION ACCESS
- Decentralized Security Representative (DSR) Standard.

14. INFORMATION AVAILABILITY
- Data Archiving Standard.
- Data Retention Standard.
- Data Storage Standard.

15. INFORMATION CONFIDENTIALITY
- Password Requirements Standard.
- Identity Management Standard.

16. INFORMATION CONTENT
- System and Information Integrity Standard.

17. INTRUSION DETECTION SYSTEMS (IDS)
- Network Protection Standard.

18. MANAGEMENT OF REMOVABLE COMPUTER MEDIA
- Media Disposal Standard.

19. PERSONAL COMPUTER USAGE
- Personal Device Standard.
- System Acceptable Use Standard.

20. PHYSICAL AND ENVIRONMENTAL SECURITY
- Physical Access Control Standard.
- Physical Security Systems Standard.

21. PROTECTION OF INFORMATION
- Data Storage Standard.
- Data Classification Security Standard.

22. PUBLICLY AVAILABLE SYSTEMS
- Web Content Management System Standard.
- Vulnerability Scanning Standard.
- Insider Threat Standard.

23. REMOVABLE MEDIA
- Removable Media Usage Standard.

24. SECURITY PROGRAM MANAGEMENT
- Security Services Standard.

25. SEGREGATION OF DUTIES
- Information Systems Segregation Standard.

26. SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES
- DevOps Standard.
- Development – Continuous Integration and Continuous Delivery Standard.

27. USE OF SYSTEM UTILITIES
- Use of System Utilities Standard.
- Administrator Account Standard.
- Security Services Standard.

28. TELECOMMUNICATION SECURITY
- Network Acceptable Use Standard.
- Removable Media Usage Standard.
- Personal Device Standard.

APPENDIX A: REVISIONS

This document is to be reviewed at least once per fiscal year. If operational need or system/environmental changes require more frequent changes, these are permitted if the annual cadence does not drop below once per year.

Version Number	Change Request Number (if applicable)	Accepted Date	Author	Summary of Changes
2.0	N/A		Cyber Command	Document rewrite. Removed all sections not part of Information Security. Condensed summary information and provided links to published standard. Corrected formatting.