State of Ohio IT Standard	
Standard Number: **ITS-SEC-02**	**Title:** **Enterprise Security Controls Framework**
Effective Date: 08/27/2018	**Issued By:** Ervan D. Rodgers II, Assistant Director/State Chief Information Officer Office of Information Technology Department of Administrative Services
Version Identifier: 2.0	**Published By:** Office of Information Security & Privacy

1.0 Purpose

This state IT standard specifies the minimum requirements for information security in all agencies and identifies the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (current, published version), "Security and Privacy Controls for Federal Information Systems and Organizations," as the framework for information security controls implementation for the state.

2.0 Scope

Pursuant to Ohio Administrative Policy IT-01, "Authority of the State Chief Information Officer to Establish Ohio IT Policy," this state IT standard is applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted. Non-participating agencies are encouraged to comply with this standard as well as all enterprise policies, standards and guidelines.

3.0 Background

The State of Ohio has adopted NIST SP 800-53 (current, published version) as the information security controls framework for the state.

Adoption of this common framework of information security controls offers several advantages:

- Agencies can share a common vocabulary and common set of concepts related to information security controls, which will improve communication and understanding of this topic within and among the agencies.

- Agencies will be able to share expertise, documentation, training materials, and processes, which will allow for more cross-agency collaboration.

- A common standard can be established for auditing and common methods established for compliance monitoring.

- When everyone is using the same information security controls framework, greater insight is provided into the overall security posture of the state, which can help determine the most efficient and effective deployment of security resources.

- Using NIST SP 800-53 (current, published version) as its security controls framework, allows the state to leverage research already performed and implementation guidance already produced by the federal government and provides the opportunity for better alignment between state and federal security requirements.

The complexity involved in securing agency systems can be enormous and focus is necessary to ensure that limited resources are prioritized and applied to the areas of highest risk. Significant work has been done to address this concept and the result is the Center for Internet Security (CIS) Controls. The CIS Controls complement the security controls in NIST SP 800-53. The controls identified in the CIS Controls address the highest threat areas for the enterprise environment.

4.0 Standard

State agencies shall use NIST SP 800-53 (current, published version), as the basis for selecting information security controls. The selection and implementation of individual controls shall be based upon ***system classification*** and an overall understanding of the risks posed to that system.

To establish an information security baseline across all state agencies and address the currently known, high-priority attacks, agencies are required to implement the enterprise controls listed below.

4.1 Enterprise Controls

Agencies shall work with the Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) to implement enterprise security controls and shall leverage enterprise IT security services unless granted an exception by the DAS Office of Information Security and Privacy (OISP) (refer to section 5.0 Procedures).

4.1.1 Inventory and Control of Hardware Assets

Agencies shall maintain an up-to-date inventory of authorized devices that are permitted to connect to the agency's network and shall develop processes to detect and prevent unauthorized devices from gaining access, consistent with the guidance in the CIS Controls.

4.1.2 Inventory and Control of Software Assets

Agencies shall maintain an up-to-date inventory of authorized software and shall develop processes to detect and prevent the installation of unauthorized software, consistent with guidance in the CIS Controls.

4.1.3 Continuous Vulnerability Management

Agencies shall develop policies and procedures that are consistent with the guidance in the CIS Controls and in the risk assessment (RA) family of controls in NIST SP 800-53 (current, published version). Agencies shall utilize the enterprise vulnerability assessment services offered by DAS OISP. DAS and agencies shall share responsibility for the remediation of vulnerabilities on ***DAS-managed information systems*** as outlined in service level agreements.

4.1.4 Controlled Use of Administrative Privileges

Agencies shall implement controls for the assignment, use, and configuration of administrative privileges consistent with the guidance in the CIS Controls.

4.1.5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Agencies shall adopt and actively maintain common hardware and software configurations on mobile devices, laptops, workstations, and servers, with documented security configurations, consistent with the guidance in the CIS Controls.

DAS OISP provides all state agencies with access to the CIS Benchmarks, which offer secure baseline configurations for common laptop, workstation, and server operating systems (refer to section 5.0 Procedures).

4.1.6 Maintenance, Monitoring, and Analysis of Audit Logs

Agencies shall implement auditing and logging capabilities and procedures to help detect, understand, or recover from an attack. Agencies shall forward system and/or audit logs to the enterprise security information and event management (SIEM) solution.

4.1.7 E-mail and Web Browser Protections

Agencies shall first employ DAS OIT provided e-mail and web browser controls. Agencies shall consult with DAS OIT to implement supplemental controls within their environment based on their risk profile. Agencies shall use supported e-mail clients and web browsers.

4.1.8 Malware Defenses

Agencies shall utilize the enterprise anti-malware services that are offered by DAS OISP, which are configured according to the guidance in the CIS Controls.

4.1.9 Limitation and Control of Network Ports, Protocols, and Services

Agencies shall identify and enable only necessary network ports, protocols and services based on validated business needs. Agencies shall periodically review existing ports and services to ensure that the need remains. Where DAS manages systems for an agency, the agency shall work with DAS OIT to implement this control.

4.1.10 Data Recovery Capabilities

Agencies shall develop data backup and recovery plans based on the business needs of the system, and work with DAS OIT to implement and

validate these plans on DAS-managed information systems. These data backup and recovery plans shall include regular, automated backups; regular tests of backup procedures; protection of backups physically and through encryption; and retention of at least one offline backup to mitigate against malware.

4.1.11 Secure Configuration for Network Devices such as Firewalls, Routers, and Switches

Agencies shall adopt and document standard secure configurations for all network devices deployed within the agency. Agencies shall adopt security configurations of network devices. All configuration changes shall be documented and approved via a formal change control process. Automated tools shall be used to verify configurations, detect changes, and alert security personnel of changes. Devices shall be managed using multi-factor authentication and an encrypted session. The latest stable version of any security update shall be installed on all network devices. A management virtual local area network (VLAN) shall be established to separate network management traffic from business traffic.

4.1.12 Boundary Defense

DAS OIT shall implement an intrusion detection system (IDS) at the network boundary, and a web filtering solution. Agencies may implement additional boundary defenses, such as, but not limited to data loss prevention (DLP) systems in consultation with DAS OIT.

4.1.13 Data Protection

Agencies shall adopt practices to protect the ***confidentiality*** and ***integrity*** of ***sensitive data***, consistent with the CIS controls. DAS OIT shall implement data protection controls on enterprise cloud services, such as SharePoint Online and OneDrive, to protect the confidentiality and integrity of sensitive data. These include, but are not limited to, protecting data in use; data in motion, and data at rest. Refer to Ohio Administrative Policy IT-14, “Data Encryption and Securing Sensitive Data,” for additional requirements.

4.1.14 Controlled Access Based on the Need to Know

Agencies shall implement access controls based upon the principles of need to know and least privilege, consistent with the guidance in the CIS controls and the access control (AC) family of controls in NIST SP 800-53 (current, published version).

4.1.15 Wireless Access Control

Agencies shall implement controls to protect wireless devices, which are consistent with the guidance in the CIS controls. Agencies shall first utilize the enterprise wireless as a service (WaaS) offering to implement and protect wireless local area networks (LANs), wireless access points, and wireless client systems.

4.1.16 Account Monitoring and Control

DAS OIT shall establish enterprise controls to manage the lifecycle for system and application accounts. Agencies shall implement controls to

monitor and control agency maintained system and user accounts consistent with the guidance in the CIS controls.

4.1.17 Implement a Security Awareness and Training Program

Agencies shall comply with the requirements outlined in Ohio Administrative Policy IT-15, "IT Security Awareness and Training."

4.1.18 Application Software Security

Agencies shall implement application security controls consistent with the guidance in the CIS controls.

4.1.19 Incident Response and Management

Agencies shall report security and privacy ***incidents*** to DAS OIT immediately upon discovery, and fully cooperate with the DAS OISP Security Incident Response Team. Refer to the OIT Enterprise Procedure OEP-SEC.4001, "Statewide Incident Response Reporting," for additional details.

DAS OISP shall establish incident response and management capabilities to effectively and efficiently handle security incidents. Agencies shall also develop their own internal incident response procedures. Due to the sensitive nature of incident response and investigation, agencies shall involve their chief legal counsel as well as human resources in these procedures. Additionally, DAS OISP and agency incident response procedures shall be tested annually.

4.1.20 Penetration Tests and Red Team Exercises

DAS OISP shall provide penetration testing on a periodic basis to ensure effectiveness of implemented controls. Agencies shall perform or sponsor additional penetration testing on a periodic basis to ensure the effectiveness of implemented controls.

Additionally, agencies shall consider having external teams perform exercises to further assess the efficacy of their defenses consistent with the guidance in the CIS Controls.

5.0 Procedures

5.1 Exception Process: To request an exception to one or more of the requirements outlined in this standard, please complete an IT Security Exception Request form**.**

5.1.1 The form is located within the IT Enterprise Services Portal under the "Services & Products" category.

5.1.2 If you have any questions, please contact DAS OISP (refer to Section 9.0 Inquiries for contact information).

5.2 Obtaining CIS Benchmark Resources

Any user with an e-mail address that ends in "ohio.gov" or "state.oh.us," has the ability to login into the CIS website and create a CIS ID. From there, users can access or download the available CIS benchmarks and participate in related

technical communities. Visit https://workbench.cisecurity.org/login to create an account.

For questions or for additional information, please contact DAS OISP (refer to Section 11.0 Inquiries for contact information).

6.0 References

6.1 Ohio Administrative Policy IT-01, *Authority of the State Chief Information Officer to Establish Ohio IT Policy,* defines the authority of the state CIO to establish State of Ohio IT standards as they relate to the acquisition and use of information technology by state agencies, including, but not limited to, hardware, software, technology services and security.

6.2 Ohio Administrative Policy IT-14, *Data Encryption and Securing Sensitive Data*, outlines the requirements for identifying and securing sensitive data as well as the devices and media on which sensitive data resides.

6.3 Ohio Administrative Policy IT-15, *IT Security Awareness and Training*, provides IT security awareness and training requirements for State of Ohio information system users, which includes employees, contractors, temporary personnel and other agents of the state.

6.4 OIT Enterprise Procedure OEP-SEC.4001, *Statewide Incident Response Reporting*, defines the steps to be followed by State of Ohio agencies reporting information, computer system, privacy or network security incidents.

6.5 NIST Special Publication 800-53 (current, published version), *Security and Privacy Controls for Federal Information Systems and Organizations*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

6.6 *Center for Internet Security (CIS) Controls*, a set of baseline security controls that are effective in blocking high-priority attacks. Organizations must implement these controls as a first step toward improving cyber defense.

7.0 Definitions

Availability	Ensuring timely and reliable access to and use of information.[1]
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [2]
DAS-managed Information System	Information systems that reside in facilities or infrastructure managed by DAS OIT personnel. Primary responsibility for managing these systems may be assigned to DAS OIT personnel or other outside entities.

[1] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
[2] *Ibid.*

Incident

A security incident threatens the confidentiality, integrity or ***availability*** of state information resources. Some examples of incidents include:

- Loss or theft of a computing device or media (e.g., laptop, smartphone, storage device, authentication token)
- Denial of Service (DoS)
- Improper system usage or access
- Information spillage
- Malicious code (e.g., virus, worm, Trojan horse)
- Phishing messages
- Social engineering

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.[3]

Personally Identifiable Information

"Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

Sensitive Data

Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of ***personally identifiable information*** that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, Criminal

[3] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy, and the Social Security Administration Limited Access Death Master File. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

System Classification — Refers to the process of assessing the potential impact to confidentiality, integrity and availability of the evaluated system. In the NIST SP 800-53 publication they refer to FIPS-199, which are the federal guidelines for assessing and classifying information systems.

8.0 Related Resources

Document Name
FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems is available at the following location: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and other NIST Special Publications of interest to the information security community can be found at the following location: http://csrc.nist.gov/publications/PubsSPs.html
Center for Internet Security (CIS) Controls are available at the following location: https://www.cisecurity.org/controls/

9.0 Implementation

Due to the length of time that this standard has been in effect, state agencies should already be in alignment with the requirements. The revisions capture current statewide IT security practices. For compliance related questions, please contact DAS OISP (refer to section 11.0 Inquiries for DAS OISP contact information).

10.0 Revision History

Revision Date	Description of Changes
04/18/2011	Version 1.0, original standard
08/27/2018	Version 2.0, updated references from CAG to the CIS Controls. In addition, revised the requirements to address the implementation of enterprise IT security services and to reflect current State of Ohio IT security practices.
11/29/2018	Updated the exception request language to align with the current procedure.
01/15/2020	Updated standard template.
01/15/2021	Scheduled standard review.

11.0 Inquiries

For information regarding this state IT standard or the NIST Special Publication 800-53 security controls framework, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor
Columbus, Ohio 43215

Telephone: 1-614-644-9391
Email: state.isp@das.ohio.gov
Web: infosec.ohio.gov

State of Ohio IT Standards can be found online at:
https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards

12.0 Attachments

None.