State of Ohio Administrative Policy

No:

Information Technology
IT-01

Effective:

May 21, 2020

Issued By:

Matthew M. Damschroder, Director

Authority of the
State Chief Information Officer
to Establish Ohio IT Policy

1.0   Purpose

The purpose of this policy is to communicate the information technology (IT) policy-making authority of the state chief information officer (state CIO), who is also the assistant director for the Ohio Department of Administrative Services (DAS). Under the direction of the director of DAS, the state CIO shall establish policies and standards for the acquisition and use of common information technology by state agencies, including, but not limited to, hardware, software, technology services, and security, and the extension of the service life of information technology systems, with which state agencies shall comply.[1]

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in **_bold italics_**.

2.0   Policy

Under the authority and within the limits set forth in the Ohio Revised Code (ORC), and the Code of Federal Regulations, the state CIO, under the direction of the director of DAS, has been granted policy authority as it relates to the acquisition and use of telecommunications and information technology, including, but not limited to, hardware, software, technology services, information security and privacy (including the protection of **_sensitive data_** and **_personally identifiable information_**), and the extension of the service life of information technology systems. This policy authority is promulgated in five distinct forms - administrative rules, policies, standards, procedures and bulletins (see Attachment 1). Each has its own enumeration scheme (see Attachment 2).

2.1   **Ohio IT Administrative Rules**: Administrative rules are written statements of law adopted by an administrative agency pursuant to authority granted under the ORC to carry out the policies and intent of a statute enacted by the General Assembly.

---

[1] As outlined in Ohio Revised Code Section 125.18.

Ervan D. Rodgers II, State Chief Information Officer
Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

614-466-6930
State.ITPolicy.Administrator@oit.ohio.gov

Administrative rules are codified in the Ohio Administrative Code once they are adopted. The state CIO establishes IT-related administrative rules. The DAS Office of Information Technology (OIT) administrator for Enterprise IT Architecture & Policy (EITAP), the chief information security officer (CISO), and/or the chief privacy officer (CPO) administer their drafting and promulgation. The Secretary of State and the Ohio Legislative Service Commission maintain official registers of Ohio administrative rules. Established rules are available at the Ohio General Assembly Web site at https://www.legislature.ohio.gov/laws/ohio-codes. Pending or newly adopted rules are published in the Register of Ohio at www.registerofohio.state.oh.us.

2.2   **Ohio IT Policies**: Policies are statements of specific management direction established by the state CIO as necessary to ensure that investment in and use of information technology by state agencies produces the best solutions for the state as a whole and its respective agencies. Such policies are written in a standardized format and contain an effective date after which the policy is operational. Policies do not have an expiration date. They are updated or rescinded as needed. The state CIO establishes IT-related state policies. The DAS OIT administrator for EITAP, the CISO, and/or the CPO administer their drafting. The DAS OIT administrator for EITAP is responsible for promulgation and maintains the official register of Ohio IT Policy, which is published at www.das.ohio.gov/forStateAgencies/Policies.aspx.

2.3   **Ohio IT Standards**: Standards are statements of specifically prescribed use and acquisition established by the state CIO as necessary to produce the best IT solutions for the state as a whole and its respective agencies. Ohio IT standards are written in a standardized format and contain an effective date for compliance. Ohio IT standards do not have an expiration date. They are updated or rescinded as needed. The state CIO establishes state IT-related standards. The DAS OIT administrator for EITAP, the CISO, and/or the CPO administer their drafting. The DAS OIT administrator for EITAP is responsible for promulgation, and maintains the official register of State of Ohio IT Standards, which is published at https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards.

2.4   **Enterprise IT Procedures**: Enterprise IT procedures are statements of the specific steps or a course of action that state agencies and other entities external to DAS OIT must follow:

- to obtain a DAS OIT-provided service; or
- in interacting with DAS OIT in its efforts to carry out its coordination and oversight role as mandated by the ORC; or

- to comply with an Ohio IT administrative rule, policy, standard or bulletin.

Enterprise IT procedures are written in a standardized format and contain an effective date for compliance. Enterprise IT procedures do not have an expiration date. They are updated or rescinded as needed. The state CIO, CISO, CPO, administrator for EITAP or any DAS OIT business unit manager or service owner shall direct the drafting and promulgation of procedures assigned to their respective areas. The DAS OIT administrator for EITAP administers a publication process, and maintains the official register of Enterprise IT Procedures, which is published at https://das.ohio.gov/Divisions/Information-Technology/Ohio-Enterprise-IT-Procedures.

2.5 **IT Bulletins**: Bulletins are established by the state CIO to communicate highly relevant and timely direction that may: address problems or questions of a temporary, one-time, or quickly emerging nature; draw attention to regulations affecting a project of particular interest; clarify administrative rules, policies, standards or procedures; or require compliance in anticipation of a pending IT administrative rule, policy, standard or procedure. IT bulletins may or may not require compliance and will be so noted. IT bulletins are written in a standardized format and contain an issue date. They may have an expiration date, be superseded by an Ohio IT administrative rule, policy, standard or procedure, or be updated or rescinded as needed. The state CIO establishes state IT-related bulletins. The DAS OIT administrator for EITAP, CISO, and/or CPO administers their drafting. The DAS OIT administrator for EITAP is responsible for promulgation, and maintains the official register of State of Ohio IT Bulletins, which is published at https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Bulletins.

3.0 Authority

Chapters 125, 175, 187, 1306, 1347, 3334 and 3353 of the Ohio Revised Code; and Title 41 Part 102-173 of the Code of Federal Regulations

4.0 Revision History

Date	Description of Change
07/1/1991	OPP-001 replaces all prior memoranda regarding this topic.
08/9/2001	Updated to incorporate the authority given to DAS to adopt administrative rules and publish recommendations regarding legally binding electronic transactions and the use of electronic signatures.
09/26/2001	ITP policy ITP A.1 supersedes ITP policy OPP-001: A new numbering system and a new policy format have been introduced.
10/03/2001	Updated policy to reflect office name change from the Office of IT Policy and Planning (OPP) to the Office of Statewide IT Policy (ITP).

09/06/2006	Updated policy to include reference to ORC 125.18 and Executive Order 2004-02T, reflect the change of authority from DAS to OIT, and include the authority to issue official state IT standards and OIT enterprise procedures.
03/22/2007	Updated policy to reflect the rescission of Executive Order 2004-02T.
10/13/2016	Updated to reflect changes in procurement authority. Transferred policy content to a new State of Ohio Administrative Policy Template. Re-numbered policy to IT-01 to be consistent with new numbering format.
05/21/2020	Updated to clarify the scope of policy-making authority as well as roles and responsibilities.
05/21/2022	Scheduled policy review.

5.0 Inquiries

Direct inquiries about this policy to:

> State IT Policy Manager
> Enterprise IT Architecture & Policy
> Office of Information Technology
> Ohio Department of Administrative Services
> 30 East Broad Street, 39th Floor
> Columbus, Ohio 43215
>
> 1-614-466-6930 | DAS.State.ITPolicy.Manager@das.ohio.gov

State of Ohio Administrative Policies may be found online at
https://das.ohio.gov/Divisions/Administrative-Support/State-Administrative-Policy

6.0 Attachments

Attachment 1 – Table of Responsibility. This attachment outlines responsibilities for the five distinct types of official Ohio IT-related policy.

Attachment 2 – Table of Enumeration. This attachment provides the enumeration scheme for each of the five distinct types of official state IT-related policy.

Appendix A – Definitions

a. Personally Identifiable Information (PII). "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.

b. <u>Sensitive Data</u>. Sensitive data is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted. 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 data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. Examples include, but are not limited to, Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, Criminal 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 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.

Appendix B - Resources

Document Name
Ohio Revised Code: http://codes.ohio.gov/orc
Ohio Administrative Code: http://codes.ohio.gov/oac
Ohio IT administrative rules, policies, standards, bulletins, procedures, guidelines & best practices: https://das.ohio.gov/Divisions/Information-Technology

Attachment 1

Table of Responsibility

Type	Authority From	Issued By	Published By	Compliance Required	Applicability
Ohio Administrative Rules	**General Assembly** Ohio Revised Code Sections 111.15, 119.03,125.02, 1306.20, 1306.21 and 1347.06	**State CIO following review by the General Assembly**	**Ohio Legislative Service Commission and the Ohio Secretary of State**	**Yes**	Varies as established by the Ohio Revised Code, though generally more expansive in scope than for Ohio IT policies and standards.
Ohio IT Policies	**General Assembly** Ohio Revised Code Sections 125.18, 4121.121 **U.S. General Services Administration** 41 CFR Part 102-173	**DAS Director**	**DAS OIT Administrator for EITAP**	**Yes**	Policies written under ORC Sections, 125.18, 175.12, 187.03, 3334.08 and 3353.04 are applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government, other than any state-supported institution of higher education, the office of the auditor of state, treasurer of state, secretary of state, or attorney general, the adjutant general's department, the bureau of workers' compensation, the industrial commission, the public employees retirement system, the Ohio police and fire pension fund, the state teachers retirement system, the school employees retirement system, the state highway patrol retirement system, the general assembly or any legislative agency, the capitol square review and advisory board, the courts or any judicial agency, the Ohio housing finance agency, the Ohio tuition trust authority, the JobsOhio Corporation, or the broadcast educational media commission. Pursuant to sections 125.02, 125.04, 125.041, 125.18, 175.12, 187.03, 3334.08 and 3353.04 of the ORC, provisions of state IT policies concerning the procurement of IT products and services apply to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government, other than any state-supported institution of higher education, the office of the auditor of state, treasurer of state, secretary of state, or attorney general, the adjutant general's department, the industrial commission, the public employees retirement system, the Ohio police and fire pension fund, the state teachers retirement system, the school employees retirement system, the state highway patrol retirement system, the general assembly, the capitol square review and advisory board, the courts or any judicial agency, the Ohio housing finance

Type	Authority From	Issued By	Published By	Compliance Required	Applicability
					agency, the Ohio tuition trust authority, the broadcast educational media commission and the JobsOhio Corporation. State and local policies written under 41 CFR Part 102-173 are applicable to every organized body, office or agency established for the exercise of any function of state or local government in Ohio regarding the registration and use of the .gov domain.
Ohio IT Standards	**General Assembly** Ohio Revised Code Sections 125.18, 175.12, 187.03, 3334.08 and 3353.04 **U.S. General Services Administration** 41 CFR Part 102-173	**State CIO**	**DAS OIT Administrator for EITAP**	**Yes**	Same as for Ohio IT Policies (see above).
Enterprise IT Procedures	**General Assembly** Ohio Revised Code Section 125.18 **U.S. General Services Administration** 41 CFR Part 102-173	**State CIO, CISO, CPO, DAS OIT Administrator for EITAP or any other business unit manager or service owner**	**DAS OIT Administrator for EITAP**	**Yes**	State agencies and other entities external to DAS OIT must follow Enterprise IT Procedures: • to obtain a DAS OIT-provided service; or • in interacting with DAS OIT in its efforts to carry out its coordination and oversight role as mandated by ORC; or • to comply with an Ohio IT policy, standard or administrative rule. If an agency that is otherwise exempted from DAS OIT authority purchases rated services administered by DAS OIT, or acquires or uses a product or service subject to a state contract administered by DAS OIT, or otherwise participates in an initiative administered by DAS OIT, then Enterprise IT Procedures relating to that service, product or initiative may or may not apply and are so noted.
Ohio IT Bulletins	**General Assembly** Ohio Revised Code Sections 125.18, 175.12, 187.03, 3334.08 and 3353.04 **U.S. General Services Administration** 41 CFR Part 102-173	**State CIO**	**DAS OIT Administrator for EITAP**	**Depends** It is the nature of IT bulletins that they may or may not require compliance.	Depends – If compliance is required, the application of an IT bulletin may be specified as the same as for Ohio IT policies, standards or OIT enterprise IT procedures (see above).

Attachment 2

Table of Enumeration

Type	Enumeration
Ohio Administrative Rules	Rule 123:3-#-##
Ohio IT Policies	IT- ##
Ohio IT Standards	ITS-[Domain ID]^2-##
Enterprise IT Procedures	OEP-[Division ID]^3.####
Ohio IT Bulletins	ITB-YYYY.##

---

[2] A domain ID is a series of letters. The domain assignment is dictated by the subject matter of the standard document. NET = Network, PLF = Platform, SEC = Security, SHW = Server Hardware, SW = Software, SYS = System.

[3] The division ID is a series of three letters that identifies the issuing DAS division or functional area. (e.g., SEC = Security, IGD = Investment & Governance Division, ISD = Infrastructure Services Division)