	IT Governance Policy GV-OC-P1		
Effective Date: 09/30/2024	**Review Date:** 09/24/2024	**Version:** 1.1	**Page #:** 1 of 6

PURPOSE

The Secretary of the State of Alabama Office of Information Technology (OIT), exercising authority according to State law (refer to OIT Administrative Rules and the Code of Alabama 1975, §§ 41-4-220 et seq., §§ 41-4-280 et seq., and §§ 41-28-1 et seq.), promulgates rules, regulations, and policies and establishes procedures and standards for the management and operation of Information Technology (IT) by State agencies, including coordinating State IT; providing technical assistance to State agency administrators on design and management of State IT systems; evaluating the cost, system design, and suitability of IT equipment and related services; establishing standards and policies for project management and project methodologies; and developing a unified and integrated structure and enterprise architecture for IT systems for all State agencies.

OBJECTIVE

Create, communicate, and manage IT policies based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 R2 Risk Management Framework for Information Systems and Organizations (RMF), NIST SP 800-53 R5 Security and Privacy Controls for Information Systems and Organizations, and the NIST AI Risk Management Framework (AI-RMF) 1.0.

All assets that process, store, receive, transmit, or otherwise affect the confidentiality, integrity, and availability of State data must meet the required security controls defined in this document and all policies, standards, and procedures governed by this policy. This policy addresses the requirements set forth by the State to implement the identified security controls.

For the purposes of this and all other OIT published policies, the term “State Data” represents any data that is created and/or controlled by any State agency in support of the citizens of the State of Alabama that is not already defined as protected under federal laws, statutes, and regulations.

STATEMENT OF POLICY

All State agencies in the Enterprise will follow IT policies including this policy and all policies, standards, and procedures governed by this policy. “Enterprise” or “State agencies” is defined as all Executive Branch departments, agencies, offices, boards, commissions, bureaus, and authorities (agency or agencies) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of IT resources, including contractors and retired State employees, that are not expressly exempted from the Secretary’s authority. The terms, “shall,” “will,” and “must” are interchangeable and indicate required activity, behavior, or action within State policy.

SCOPE

This policy covers all State data, information, and information systems used, managed, or operated on behalf of the State by an agency, an agency user (employee or contractor), or other organization and applies individually and collectively to all State employees, contractors, and all other users of State data, information, and information systems that support State operations and assets.

ROLES AND RESPONSIBILITIES

All State employees, contractors, and all other users or accessors of State IT resources, data, information, and information systems are responsible for adhering to this policy and the policies governed by this policy, as well as their defined control requirements.

OIT Responsibilities:

a. Exercise authority according to State law; refer to OIT Administrative Rules and the Ala. Code §§ 41-4-220 et seq., §§ 41-4-280 et seq., and §§ 41-28-1 et seq. or as amended.
b. Create, communicate, and maintain Enterprise IT policies.
c. Provide an Enterprise IT policy lifecycle management process.

d. Monitor compliance with Enterprise IT policies.
e. Review and approve/reject agency Enterprise IT policy exemption requests or appeals.
f. Ensure Enterprise IT policies are reviewed periodically.

Agency Responsibilities:

a. Follow Enterprise IT policies.
b. Ensure agency IT policies are equally or more restrictive / protective than the corresponding Enterprise IT policies.
c. Ensure users follow Enterprise IT policies.
d. Protect information, data, and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
e. Make Enterprise IT policy exemption or exception requests to OIT.

User Responsibilities:

a. Follow Enterprise IT policies.
b. Immediately notify their manager and email OIT, at service.desk@oit.alabama.gov, to report a known or perceived policy violation. Include in the subject of the email the policy that is potentially being violated.

Third-Party Responsibilities:

a. Ensure all IT systems and applications developed for the State conform to this policy and other Enterprise IT policies and standards.
b. Non-conforming IT systems cannot deploy unless the purchasing entity and their contractor have jointly applied for and received, in writing from the Secretary of OIT, or the Secretary's designee, an authorization to operate (ATO) or notice that a specified exception will be permitted.

CONTROL APPLICATION

Security controls governed by this policy must be applied to data and the associated asset(s) where the information is processed, transmitted, or stored based on the following data classification definitions. Control requirements above what is currently provided in State policies will be the responsibility of the individual agency(ies). Below are the categories of information with a description of the information involved, level of risk attached, data types to be considered (not an exhaustive list), and the applicable control level.

Public:

a. Risk Level – No Risk
b. Description – Information declared public knowledge by someone with the authority to do so and can freely be given to anyone without any possible damage to the State or to any individual. Disclosure of public information should be expected to have no adverse effect on State operations, State assets, or individuals made confidential by State or Federal law.
c. Data Type(s) – Information on publicly accessible websites
d. Applicable Control Level – Moderate

Internal:

a. Risk Level – Low Risk
b. Description – Information intended primarily for employees of the State (personnel information, descriptions of work processes, information technology standards and procedures, etc.) shall be limited to internal distribution. The unauthorized disclosure of internal information could be expected to have a limited adverse effect on State operations, assets, or individuals.
c. Data Type(s) – Routine correspondence, email, and other internal documents
d. Applicable Control Level – Moderate

Sensitive:

a. Risk Level – Medium Risk
b. Description – Sensitive information includes (but is not limited to) personally identifying information (such as that specified in Ala.Code § 8-38-2(6) which includes date of birth, social security number, driver's license number, etc.), and other personal information that could undermine individual integrity (personnel records, disciplinary action records, etc.). This category also includes Protected Health Information (PHI) as defined by the Health Information Portability and Accounting Act (HIPAA) of 1996 or Federal and State regulations. The unauthorized disclosure of sensitive information could be expected to have a serious adverse effect on State operations, assets, or individuals.
c. Data Type(s) – Confidential personnel records, Trade Secrets, Security Features, Sensitive Public Security Information, Family Educational Rights and Privacy Act
d. Applicable Control Level – Moderate

Confidential:

a. Risk Level – High Risk
b. Description – Information that must be protected to ensure the security of State residents and resources. Confidential information may include data pertaining to State infrastructure (utilities and services), records of legal proceedings, and data protected as evidence. The unauthorized disclosure of confidential information could be expected to have a severe or catastrophic adverse effect on State operations, State assets, or individuals.
c. Data Type(s) – Banking Regulatory Information, Payment Card Industry Data Security Standards, Criminal Justice Information, State and Federal Tax Information, Social Security Administration Provided Information
d. Applicable Control Level – Moderate and Privacy Controls

COMPLIANCE

Compliance with this policy and the policies, standards, and procedures governed by this policy is required. The following shall be used to ensure effective policy compliance:

a. Suspension from State IT systems.
b. Termination or suspension of contractual agreements.
c. Denial of access to State IT resources.
d. Suspension of agency IT purchases.
e. Agency Heads and senior IT leadership shall provide to OIT (upon request) attestation indicating acknowledgement, implementation, or evidence of compliance with this policy and the policies, standards, and procedures governed by this policy.

POLICY EXEMPTIONS OR EXCEPTIONS

Requests for exemptions or exceptions to this policy and the policies, standards, and procedures governed by this policy shall be reviewed by the Secretary of OIT. State agencies requesting exemptions or exceptions shall provide such requests to the Secretary of OIT in the manner, form, and conditions established or required by the Secretary of OIT. The Secretary of OIT shall review such requests and approve or reject agency enterprise IT policy exemption or exception requests or appeals.

Requests for policy exemptions or exceptions should be sent to the OIT Service Desk (service.desk@oit.alabama.gov) and must include a completed IT Policy Exemption Request form. The form should be completed by the agency's Information Security manager (or equivalent). The form may be found in the OIT Documents Library or by following this link - OIT IT Policy Exemption Request.

POLICY REVIEWS AND UPDATES

They shall also be updated following events necessitating such change. This policy and the policies, standards, and procedures governed by this policy shall be developed, documented, and disseminated by the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

This policy and the policies, standards, and procedures governed by this policy shall be reviewed and updated at least every three (3) years or as the Secretary of OIT determines.

POLICY OWNER

Secretary, State of Alabama Office of Information Technology (OIT).

MATERIAL SUPERSEDED

This current policy supersedes all previous versions of the policy as of the Effective Date.

REVISION HISTORY

Revision Date	Summary of Change
09/24/2024	Updated formatting errors in printed copy.
07/19/2024	Initial Creation

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	09/24/2024

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK