GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exemptions or Exceptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State.

All information assets that process, store, receive, transmit, or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, Incident Response security controls.

APPLICABILITY

This document addresses the requirements set forth by the State to implement the family of Incident Response security controls at the organization, process, and/or system level for all information assets/State data and provides requirements for the Incident Response process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

IR-1 POLICY AND PROCEDURES

The State has adopted the Incident Response principles established in NIST SP 800-53 r5, "Incident Response" control guidelines as the official policy for this security domain. The "IR" designator identified in each control represents the NIST-specified identifier for the System and Information Integrity control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the Incident Response requirements the State and executive-branch agencies must implement and maintain for policy compliance.

This policy and associated procedures shall be reviewed and updated at least every three (3) years unless State-defined events require more frequent review. This policy and the associated procedures shall be developed, documented, and disseminated by the agency head, Chief Information Officer (CIO), Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

A security incident is defined as follows:

- An event/occurrence determined to have an impact on the State prompting the need for response and recovery;
- An event/occurrence that imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or information systems; or
- An event/occurrence which constitutes a violation or threat of violation of law, security policies, procedures, or acceptable use policies.

IR-2 INCIDENT RESPONSE TRAINING

Personnel with access to the State network shall be trained in their incident response roles. Incident response training must be provided to all State employees, contractors, agencies, or other organizations on behalf of the State consistent with their assigned roles and responsibilities. Organizations shall:

a. Provide incident response training prior to assuming an incident response role/responsibility or acquiring access.
b. Provide additional or supplemental incident response training when information system changes occur.
c. Provide training annually thereafter.
d. Include in incident response training materials information related to the identification and reporting of suspicious activities, both from external and internal sources.
e. Review and update incident response training content on a regular basis and/or following agency-defined events including but not limited to assessment/audit findings or guidelines changes.
f. Maintain a comprehensive record of all incident response related training, which includes participant names, information system user IDs, type of training, and completion date.

IR-3 INCIDENT RESPONSE TESTING

All incident response personnel and service providers shall perform the following testing:

a. Identify essential mission and business functions and associated incident response requirements.
b. Organizations must perform tabletop exercises using scenarios that include a breach of sensitive or confidential data and should test the organization’s incident response policies and procedures.
c. A subset of all employees and contractors with access to sensitive or confidential data must be included in tabletop exercises.
d. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.
e. Organizations entrusted with sensitive and confidential data must test the incident response capability at least annually.

IR-3 (2) INCIDENT RESPONSE TESTING – COORDINATION WITH RELATED PLANS

Organizations shall coordinate incident response testing with agency resources responsible for related plans. Agency plans related to Incident Response testing include, for example, business

continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

IR-4 INCIDENT HANDLING

Incident response capabilities are dependent on the capabilities of organizational information systems processes being supported by those systems.

Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access and network monitoring, user or administrator reports, and reported supply chain events.

An effective incident handling capability includes coordination among the various agency entities (e.g., system owners, authorizing officials, human resources offices, physical security offices, legal departments, etc.). Some examples of suspected security incidents can include, but are not limited to, the receipt of suspicious email communications that can contain malicious code and supply chain incidents including the insertion of counterfeit hardware or malicious code into information systems or system components.

The State of Alabama has created legislation[1] that states an incident that involves Personally Identifiable Information (PII) is considered a breach. A breach results in unauthorized disclosure, loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses PII or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Agencies shall ensure they create/follow an Incident Response Plan which addresses the Security Incident Response Life Cycle that includes the following (as defined in NIST SP 800-61, Computer Security Incident Handling Guide):

a. Preparation;
b. Detection and Analysis;
c. Containment, Eradication, and Recovery; and
d. Post-Incident Activities.

The IR Plan shall also include the following:

a. How the agency will coordinate incident handling activities with contingency planning activities;
b. The steps to be followed when any security incident has been reported (both logical and physical);
c. What information will be included in the investigation including its cause, if possible, and the appraisal of its impact on systems, data, and/or personnel. The extent of damage must be determined, and course of action planned and communicated to the appropriate parties. All evidence relating to the security incident shall be collected and preserved according to State and federal requirements, including but not limited to a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions resulting from the incident;
d. The creation of an Incident Response Team (IRT) to act on behalf of the CISO and/or executive leadership to decide which agency resources are required to best respond to and mitigate a security incident. If a security incident is identified by OIT, OIT will lead an IRT with representation from the affected agencies and any law enforcement representatives (if applicable). If a security incident is identified by an agency, the agency will lead the IRT and include a representative of OIT in its membership;

e. The reporting structure for all information related to the incident investigation, including final findings;

f. That lessons learned from ongoing incident handling activities, which will be incorporated into incident response procedures, training, and testing, and any resulting changes will be implemented accordingly;

g. That records of information security breaches and the remedies used for resolution shall be maintained as references for evaluating any future security breaches. The information shall be logged and maintained for at least three (3) years in a location in which it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned; and

h. The assurance that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization to ensure incident handling consistency of logistics, communications, coordination, and planning functions to resolve an incident in a structured and efficient manner.

Agencies shall establish controls to protect data integrity and confidentiality during investigations of information technology security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure fraudulent activities requiring collusion do not occur.

Any system, network, or security administrator observing malicious user activity on the State network or system shall take appropriate action to disable the user's account.

In the event of an active incident, agency management, including OIT, has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident. It may be necessary to isolate from the network until the extent of the damage can be assessed.

All personnel directly involved with incident handling must sign a Non-Disclosure Agreement (NDA) due to the sensitivity of incident details.

IR-4 (1) INCIDENT HANDLING – AUTOMATED INCIDENT HANDLING PROCESSES

Automated mechanisms supporting incident handling processes, including online incident management systems and tools that support the collection and correlation of live response data, shall be implemented, such as a Security Information and Event Management (SIEM) technology.

IR-5 INCIDENT MONITORING

Maintaining records about each information system incident, incident status, and other pertinent information is necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including, but not limited to incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Information system security incidents potentially affecting the confidentiality of any internal, sensitive, or confidential data shall be tracked, documented, and reported to agency management and OIT.

The release of confidential security information during a security incident or investigation shall be monitored and controlled to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel, or human resources.

A follow-up report shall be submitted to agency management upon resolution by those directly involved in addressing the incident and will contain the following:

a. Point of contact;
b. Affected systems and locations;
    i. System description, including hardware, operating system, and application software
    ii. Type of information processed
c. Personnel involved (if known or identified);
d. Incident description;
e. Incident resolution status;
f. Damage assessment, including any data loss or corruption;
g. Organizations contacted;
h. Corrective actions taken; and
i. Lessons learned.

IR-6 INCIDENT REPORTING

Security incidents, including suspicious events (e.g., insider threat), abnormal software errors or weaknesses, system vulnerabilities associated with security incidents (e.g., Ransomware), and lost or stolen State computer equipment shall be reported immediately to the OIT Service Desk at 334-242-2222. The Service Desk will forward the information to the State Security Operations Center (SOC) for further analysis and appropriate action.

Agencies and vendors of the State must report any suspected security incidents or security breaches to the OIT Service Desk within twenty-four (24) hours of incident confirmation.

For incidents involving Federal Tax Information (FTI), refer to IRS 1075 Section 1.8, Reporting Improper Inspections or Disclosures, for more information on reporting requirements.

If a privacy or security incident involves the unauthorized disclosure of information received from the Social Security Administration (SSA), the State and executive-branch agencies shall notify the Systems Security Contact at the SSA Regional Office within one (1) hour of a suspected loss of Social Security data.

If a security incident is related to the State Transmission/Transfer Component (STC), which is OIT, and the agency is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one (1) hour, OIT must report the incident by contacting SSA's National Network Service Center (NNSC).

Contracts involving the storage and/or processing of State data shall identify the vendor's security point of contact (PoC).

Organizations (including contractors/vendors) using the State infrastructure shall notify OIT Security Operations immediately, or as soon as reasonably possible, of a security breach resulting in the unauthorized release of unencrypted or un-redacted records or data containing personal information with corresponding names. OIT will draft any required notification to be provided to the affected consumers in accordance with the State of Alabama Data Breach Notification Act.

Information documented about information technology security breaches shall be reported to the OIT Service Desk and contain at least the following:

- Personnel reporting incident;
- Date, time, and method of incident discovery;
- Incident description;
- Number of systems or sites involved in incident; and
- Category of potentially compromised systems/data (public, internal, sensitive, confidential).

IR-6 (1) INCIDENT REPORTING – AUTOMATED REPORTING

Automated processes shall be enacted for the purpose of reporting incidents (e.g., Security Information and Event Management (SIEM) technology).

IR-6 (3) INCIDENT REPORTING – SUPPLY CHAIN COORDINATION

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-7 INCIDENT RESPONSE ASSISTANCE

The State shall provide incident response support that offers advice and assistance to users of State and executive-branch agency-managed information systems for the handling and reporting of security incidents.

These resources may include digital forensic services, vulnerability assessments, and incident response capability. Agencies and service providers of the State shall establish and maintain a Memorandum of Understanding between its IR capability and the State's IR capability and other external, key providers of information systems.

IR-7 (1) INCIDENT RESPONSE ASSISTANCE – AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

The State shall increase the availability of incident response information and support with automated mechanisms, which can provide a push and/or pull capability for users to obtain incident response assistance.

IR-8 INCIDENT RESPONSE PLAN

The State shall develop an Incident Response Plan to determine structure of incident response capabilities and shall:

a. Provide the State with a roadmap for implementing its incident response capability.
b. Describe the structure and organization of the incident response capability.
c. Provide a high-level approach for how the incident response capability fits into the overall agency.
d. Meet the unique requirements of the organization, which relate to mission, size, structure, and functions.
e. Define reportable incidents.
f. Provide steps to be taken within the security incident response plan during and after cyberattacks.

g. Provide metrics for measuring the incident response capability within the organization by incident response management function below:

   i. Protect: e.g., risk assessment, malware protection, vulnerability management
   ii. Detect: e.g., network security monitoring and alerting
   iii. Respond: e.g., incident reporting, incident response, incident analysis

h. Sustain: e.g., MOUs and contracts, program management, security administration
i. Define the resources and management support needed to effectively maintain and mature an incident response capability,
j. Address the sharing of incident information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving sensitive or confidential data (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.
k. Be reviewed and approved by designated State or agency officials at least annually or as agency-defined events require.
l. Explicitly designate the responsibility for incident response to agency-defined roles/personnel.
m. Be revised as needed to address system/agency changes or problems encountered during plan implementation, execution, or testing.

IR plan changes must be communicated to identified State and agency officials. Final versions of IR plans will be distributed to State and agency-identified incident response personnel and protected from unauthorized disclosure and modification.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

Notes:

1 - Alabama Data Breach Notification Act of 2018 § 8-38-2 through § 8-38-12.

REVISION HISTORY

Revision Date	Summary of Change
09/13/2024	Policy Update

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	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK