

STATE OF ALABAMA

Information Technology Policy

POLICY 604-01: CYBER SECURITY INCIDENT RESPONSE

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

OBJECTIVE:

Ensure the State is prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Individual Information Technology User:

All users of State of Alabama computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

Information Services Division (ISD):

Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Incident response support resources may include, for example, the ISD Help Desk, a response team (described below), and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The CSIRT shall consist of members of the State IT Security Council and key personnel from other agencies as required. CSIRT responsibilities shall be defined in the Cyber Security Incident Reporting Procedures.

Agency Management, Information Technology Organization:

Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Organizations that support information systems shall develop incident response plans and/or procedures that:

- Provides the organization with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability
- Provides a high-level approach for how the incident response capability fits into the overall organization
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents

- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by designated officials within the organization

Review incident response plans and procedures at least annually.

Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

Distribute copies of the incident response plan/procedures to incident response personnel.

Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Organizations shall test the incident response capability for the information systems they support at least annually. Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinate incident handling activities with contingency planning activities.

Incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises.

Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

SUPPORTING DOCUMENTS:

- Information Technology Procedure 604P1: Cyber Security Incident Reporting
- Information Technology Procedure 604P2: Cyber Security Incident Handling

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
604-00	06/16/2011	Combines and replaces Policy 600-04 and Standard 600-04S1
604-01	07/19/2012	Reorganized requirements under Agency Responsibilities, and updated consistent with NIST 800-53 and 800-61 guidance