STATE OF ALABAMA

Information Technology Policy

Policy 600-04: Cyber Security Incident Response

OBJECTIVE:
Ensure the State is prepared to respond to cyber security incidents.

SCOPE:
This policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

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

Cyber Security Incident Response Procedures shall be developed to ensure management and key personnel are notified of cyber security incidents as required. Procedures shall designate a single point of contact for reporting all cyber security incidents.

A Cyber Security Incident Response Team (CSIRT) shall be established and supported 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 Response Procedures.

The CSIRT shall manage ongoing communications aspects of an incident in accordance with cyber security incident response procedures and State information dissemination policy.

All cyber security incidents shall be documented. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.

By Authority of:

Chief Information Officer — Date: 3/24/06

Policy History

Version	Release Date	Comments
Original	3/24/2006	