	Georgia Technology Authority	
Title:	**Incident Response and Reporting**	
PSG Number:	**SS-08-004**	
Effective Date:	**03/31/2008**	**Review Date: 05/05/2023**
Synopsis:	Sets minimum requirements for information security incident response and reporting	

PURPOSE

In support of state policy Computer Security Incident Management, each State agency must implement an information security incident handling capability. This standard establishes the minimum incident response and reporting requirements.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(9) – *State Government, Georgia Technology, General Powers*

O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*

PM-04-001 – *Information Technology Policies, Standards and Guidelines*

PS-08-005 – *Enterprise Information Security Charter*

STANDARD

Each agency must implement an incident management capability including documented processes and procedures for monitoring, detection, data collection, analysis, containment, recovery, response, reporting and escalation.

All incident response, reporting, and escalation procedures must be formally documented and approved by the State Chief Information Security Officer with review by the GBI.

Each agency must train its employees on how to recognize and report incidents in accordance with the reporting and escalation procedures.

Agencies must have a designated incident management point of contact.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Malicious Code Incident Prevention (SS-08-033)
Computer Security Incident Management (PS-08-04)

REFERENCES

NIST SP 800-61 Computer Security Incident Handling Guide
NIST SP 800-83 Guide to Malware Incident Prevention and Handling
NIST SP 800-28 Guidelines on Active Content and Mobile Code
NIST SP 800-19 Mobile Agent Security

These documents can be found in PDF and zipped formats at
http://csrc.nist.gov/publications

TERMS and DEFINITIONS

Incident Management -the process ofdetecting,mitigating, and analyzing threats or violations of security policies and limiting their effect.

Computer Security Incident - a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices which may include, but are not limited to: widespread infections from viruses, worms, Trojan horses or other malicious code; unauthorized use of computer accounts and computer systems; technology, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure; intentional disruption of critical system functionality; intentional or inadvertent penetration of firewall; compromise of any server, including Web server defacement; exploitation of other weaknesses; child pornography; attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or national security; and violations of the State security policies or standards that threaten or compromise the security objectives of the State's data, technology or communications systems.

Events of Interest - questionable or suspicious activities that could threaten the security objectives for critical or sensitive data or infrastructure. They may or may not have criminal implications.