![GTA logo] Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Incident Response and Reporting**	
PSG Number:	SS-08-004.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 2
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Information Security Office	
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, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (policy)

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.

- All security incidents or events of interest affecting systems or data categorized as moderate or high for any of the security objectives of confidentiality, integrity, or availability must be reported to the GTA Command Center within 24 hours of detection. 404-656-7378 for the Metro Atlanta area or 1-888-943-5742 if outside the Metro area.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Enterprise Malware Incident Prevention (Standard)
Computer Security Incident Management (Policy)

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 PDF formats at:
   http://csrc.nist.gov/publications/nistpubs

TERMS and DEFINITIONS

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

Computer Security Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices wich may include, but are not limited to: widespread infections from virus, worms, Trojan horse or other malicious code; unauthorized use of computer accounts and computer systems; unauthorized, 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 are 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.

Note: The PSG number was changed from S-08-004.01 on September 1, 2008