

Topics:

[Incidents](#) [2], [GTA review](#) [3] **[Incident Response and Reporting](#) [1]**

SS-08-004 Incident Response and Reporting

Issue Date: 3/31/2008

Revision Effective Date: 4/15/2014

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.

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, GUIDELINES

[Malicious Code Incident Prevention \(SS-08-033\)](#) [4]

[Computer Security Incident Management \(PS-08-004\)](#) [5]

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>[6]