

<b>Title:</b>	<b>USG Computer Security Incident Management Policy</b>		
<b>Policy Number:</b>	YYYY-Julian Date	<b>Topical Area:</b>	Security
<b>Document Type:</b>	Policy	<b>Pages:</b>	2
<b>Issue Date:</b>	DD-MMM-YY	<b>Effective Date:</b>	DD-MMM-YY
<b>POC for Changes:</b>	University System of Georgia (USG) - Office of Information Security		
<b>Synopsis:</b>	Establishes a requirement that each institution establish a process for detecting and responding to security incidents.		

## **PURPOSE**

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Through implementing solid security policies, limiting access to networks and computers, improving user security awareness, and early detection and mitigation of security risks are some the preventative actions that can be taken to reduce the risk, frequency and the cost of security incidents, not all incidents can be prevented. Therefore an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

This policy establishes the requirement for each University System of Georgia (USG) institution and the University System Office (USO) to establish an internal capability for handling computer security incidents.

## **SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS:**

The Board of Regents Policy Manual, Section 700  
USG Information Security Program Policy

## **POLICY**

Each USG institution and the USO shall establish and document an internal information security incident management capability that provides for prevention, monitoring, detection, containment, response, recovery, reporting and escalation appropriate to the level of risk and threats to the institution or USO.

USO Institutions and USO management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All USG institutions and the USO are required to report

information security incidents according to the security reporting requirements in this policy.

## **RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES**

USG Incident Response and Reporting (Standard)

## **REFERENCES**

Please see NIST Document 800-61, Computer Security Incident Handling Guide: <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 controls 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, which 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 or database server;
- exploitation of other weaknesses, known or unknown;
- child pornography;
- attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or system or national security and
- violations of the State or System security policies or standards that threaten or compromise the security objectives of the State or System's data, technology or communications systems.
- any violation of the "Appropriate Use Policy"