


| | | |
|---|---|--------------------------------|
|  Georgia Technology Authority | Georgia Technology Authority | |
| Title: | Malicious Code Incident Prevention | |
| PSG Number: | SS-08-033.01 | Topical Area: Security |
| Document Type: | Standard | Pages: 3 |
| Issue Date: | 3/31/08 | Effective Date: 3/31/08 |
| POC for Changes: | GTA Office of Information Security | |
| Synopsis: | Establishes controls to protect systems against malicious software. | |

PURPOSE

Malicious software, also known as malicious code and malware has become the most significant external threat to information systems causing widespread damage and disruption and necessitating extensive recovery efforts causing productivity and financial losses within organizations. Implementing appropriate mitigation measures will facilitate more efficient and effective malware incident prevention and response activities within state agencies

This standard establishes the minimum threat mitigation efforts required for improving malware incident prevention and response capabilities within the enterprise.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

System Owners shall incorporate policy, education and awareness as well as technical controls to mitigate the risks of incidents from malicious code in state information systems.

All state information systems shall be installed with up-to-date anti-virus software and signature files.

System owners shall implement and properly configure other appropriate technical controls to mitigate malicious code incidents such as appropriate selection, installation and configuration of operating systems, applications, firewalls and intrusion detection systems.

System owners shall monitor and conduct regular reviews of critical data and

| | |
|--------|------------------------------------|
| Title: | Malicious Code Incident Prevention |
|--------|------------------------------------|

communications systems for suspicious or unauthorized files or activity.

System Owners shall establish policies and procedures governing the use of third-party or open-source software on state information systems.

Malware prevention policies shall include provisions for remote users accessing state resources using systems within and outside the agency's control. (business partners, home computers, mobile/wireless devices etc)

Security awareness programs and incident response procedures shall incorporate specific malware prevention, recognition and reporting guidance for users and IT staff.

Responding and handling of malware incidents shall comply with the Enterprise Incident Response and Reporting standard and be included in Business Continuity Plans.

IT and security personnel shall be aware of the latest malware alerts, bulletins, and threats and the controls to mitigate the risks as they apply to their computing environments.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Protection from Malicious Software (Policy)
- Incident Response and Reporting (Standard)
- Email Virus and Content Filtering (Standard)
- Server Administration – Virus Protection for Servers (Standard)

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

TERMS and DEFINITIONS

Malware, malicious code, malicious software - refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Major forms of malware include but are not limited to: viruses, virus hoaxes, worms, Trojan Horses, malicious mobile code, blended attacks, spyware, attacker backdoors and rootkits.

| | | |
|-----------------|----------------|--------|
| Effective Date: | March 31, 2008 | 2 of 3 |
|-----------------|----------------|--------|

| | |
|--------|------------------------------------|
| Title: | Malicious Code Incident Prevention |
|--------|------------------------------------|

- Spyware malware is intended to violate a user's privacy and monitor personal activities and conduct financial fraud.
- Phishing is a non-malware threat that is often associated with malware such as using deceptive computer-based means to trick individuals into disclosing sensitive information.
- Virus hoaxes are false warnings of new malware threats.

Information System (hereafter referred to as 'system') - a discrete set of information resources (workstations, servers, applications, network, etc) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: The PSG number was changed from S-08-033.01 on September 1, 2008

| | | |
|-----------------|----------------|--------|
| Effective Date: | March 31, 2008 | 3 of 3 |
|-----------------|----------------|--------|