Topics:
malicious software [2]

Malicious Code Incident Prevention [1]

SS-08-033 Malicious Code Incident Prevention

Issue Date: 3/31/2008

Effective Date: 3/31/2008

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.

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 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 an 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 Incident Response and Reporting standard (SS-08-004) and the processes to be used shall be included in agency 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