PS-08-021 Protection from Malicious Software
Issue Date: 3/20/2008
Revision Effective Date: 3/20/2008

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 many organizations. Implementing appropriate mitigation measures should facilitate more efficient and effective malware incident prevention and response activities within state agencies.

This policy establishes the requirement for agencies to protect all state information resources from malicious software.

POLICY

System Owners shall utilize policy, education and awareness, and technical prevention and detection controls best suited for their environments, to avoid introduction and exploitation of malicious software in state information systems.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Malicious Code Incident Prevention (SS-08-033)
Incident Response and Reporting (SS-08-004)

REFERENCES

NIST SP 800-61 rev. 2 https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
NIST SP 800-83 rev. 1 https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final
NIST SP 800-28 Version 2 https://csrc.nist.gov/publications/detail/sp/800-28/version-2/final

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 toolkits.

- Spyware is malware 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.