
Topics:

[malicious software](#) [2] **Protection from Malicious Software [1]**

PS-08-021 Protections from Malicious Software

Issue Date: 3/20/2008

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 \(SS-08-033\)](#) [3]

[Incident Response and Reporting \(SS-08-004\)](#) [4]

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 toolkits.