	Georgia Technology Authority	
Title:	**Protection from Malicious Software**	
PSG Number:	**PS-08-021**	
Effective Date:	03/20/2008	**Review Date:** 08/30/2024
Synopsis:	Establishes requirements for agencies to protect all state information resources from 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 many organizations. Implementing appropriate mitigation measures should facilitate more efficient and effective malware incident prevention and response activities within state agencies.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

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.

POLICY

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

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

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

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