29.01.99.E1.23  Information Resources – Malicious Code

Approved February 5, 2004
Revised November 21, 2006
Revised September 25, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
This procedure applies to all TEES information resources which are strategic assets that must be managed as valuable state resources.

Reason for Standard Administrative Procedure
This malicious code procedure is intended to provide information to TEES information resource administrators and users to improve the resistance to, detection of, and recovery from malicious code.

Procedures and Responsibilities

1. PREVENTION AND DETECTION

1.1 For each computer connected to the network, security updates from the manufacturer of the appropriate operating system, and/or application software, must be kept current (e.g., patched and updated).

1.2 Where feasible, personal firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

1.3 Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.

1.4 Diskettes and mass storage devices will be scanned for malicious code before accessing any data on the media.

1.5 Software to safeguard against malicious code (e.g., anti-virus, anti-spyware, etc.) shall be installed and functioning on susceptible information resources that have access to the network.

1.6 Software safeguarding information resources against malicious code shall not be disabled or bypassed.

1.7 The settings for software that protect information resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software.
1.8 The automatic update frequency of the malicious code protection software shall not be altered to reduce the frequency of updates.

2. RESPONSE AND RECOVERY

2.1 All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling email.

2.2 If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software. (See also TEES SAP 29.01.99.E1.09, Incident Management.)

2.3 If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to division information resource personnel so that they may take appropriate actions in removing the malicious code and protecting other systems.

2.4 Personnel responding to the incident should have the necessary system access privileges and authority to affect the necessary measures to contain/remove the infection.

2.5 If possible, identify the source of the infection and the type of infection to prevent recurrence.

2.6 Utilize anti-viral, anti-spyware, etc. software to execute a complete system scan including the boot sector and all physical drives, to eradicate all malicious code that may be identified.

2.7 Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

2.8 Division information resource personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources.

Related Statutes, Policies, or Requirements


TEES Rule 29.01.99.E1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.09, Information Resources – Incident Management
Contact Office
Information Technology Services
(979) 847-8585