Compliance Component

DEFINITION

Name	Virus Detection and Elimination Criteria for Gateways
Description	To make available to the State of Missouri Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of Gateways.
Rationale	All Gateways within the State of Missouri computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Benefits	To significantly improve Gateway trust and security through a set of criteria for the following security services: 1. Multi-tiered virus protection. 2. Offload virus scan processing to a dedicated system. 3. Protection to Gateways from computer virus intrusion. 4. Detection of computer viruses on an infected Gateway. 5. Gateway recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Virus Detection and Elimination
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for Gateways** State of Missouri computer Gateways shall run anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. General Gateway Anti-Virus Criteria • Gateways shall be scanning for viruses continuously. • Gateway anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State of Missouri Gateways shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs

certification requires anti-virus products to detect 100% of all viruses “in the wild” as captured by the WildList Organization International (http://www.wildlist.org).

Virus Detection/Scanning Capabilities

- Anti-virus software shall be capable of detecting malicious software before it is executed.
- Shall support continuous real-time scanning capabilities.
- Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).
- Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).
- Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).
- Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).
- Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.
- Shall support both Inbound and Outbound real-time scan protection.
- Shall provide Internet Download and Content scanning for protection from suspicious web content, including:
  - o ActiveX filtering and scanning
  - o JavaScript filtering and scanning
- Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).
- Gateway anti-virus software shall have the capability to scan all major message protocols including:
  - o SMTP
  - o POP3
  - o HTTP
  - o FTP
- Gateway anti-virus software shall support SPAM detection and anti-relay (DNS based black hole lists and administrative defined anti-relay).

Internet Content Filtering

- Gateway anti-virus products shall support the filtering of web content (including POP3 email) for tailored anti-viral support including filtering on items such as:
  - o File size
  - o DNS extensions (dns.com)
  - o Web page content
  - o File extensions
  - o Multiple criteria

Virus Reporting Capabilities

- Anti-virus software shall provide remote notification of administrative alerts via the following methods:
  - o SMTP/E-Mail
  - o SNMP Alerts

- Log to a file
- Log to an Enterprise Repository

Post-Detection Virus Action Capabilities

- It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:
  - Quarantine – moving the infected file into an area where it cannot cause more harm.
  - Virus Removal – allows for repair of the damage caused by the virus.
  - Deny Access – prohibits the file from being accessed once infected.
  - Delete – complete removal of the infected file from the system.

Virus Scan Engine Update Capabilities

- Anti-virus signatures need to be updated continuously, either through a manual or automated process.
- Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily)
- Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.
- Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.

Anti-Virus Installation Criteria for Sever-based Gateways

- Anti-virus software shall be capable of automatic deployment and installation via the following:
  - Installation via image – anti-virus software shall be able to be included in the standard Gateway server image deployed within the enterprise.
  - Remote installation – Anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.
- Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.

Service and Support

- State of Missouri virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.
- Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.
- Anti-virus vendors shall provide "Virus Catalog Support" including:
  - A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.
  - Downloads or links to disinfection tools.
  - A clear and concise description of the anti-virus tools functionality, including procedures for updating the product

	with new detection signatures. o General advice to end-users on attacks and avoidance measures.		
Document Source Reference #	N/A		
Standard Organization			
Name	ISCA Labs	*Website*	www.iscalabs.com
Contact Information	ISCA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-06-2003	*Date Accepted / Rejected*	02-27-2003

Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			