



Compliance Component

DEFINITION

<i>Name</i>	Virus Detection and Elimination Criteria for Workstations
<i>Description</i>	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 workstations.
<i>Rationale</i>	All workstations 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.
<i>Benefits</i>	To significantly improve workstation trust and security through a set of criteria for the following security services: <ol style="list-style-type: none"> 1. Protection to workstation computer systems and media from computer virus intrusion. 2. Detection of computer viruses on an infected workstation system or media. 3. Workstation recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS

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

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<p>Virus Detection and Elimination Criteria for Workstations</p> <p>State of Missouri computer workstations shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.</p> <p><u>General Workstation Anti-Virus Criteria</u></p> <ul style="list-style-type: none"> • Virus scanner software shall be run on all workstations even if the networks perimeter devices are scanning for viruses. • All workstations shall be scanned for viruses at least once a day. • Workstation anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State of Missouri workstations 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 both On-Access (real-time) and On-Demand (flexible) 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:
 - ActiveX filtering and scanning
 - JavaScript filtering and scanning
- Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).

Virus Reporting Capabilities

- Anti-virus software shall provide the ability for detection notification via both audio and visual alerts.
- Anti-virus software shall provide remote notification of administrative alerts via the following methods:
 - SMTP/E-Mail
 - SNMP Alerts
 - Log to a file
 - Log to an Enterprise Repository

Post-Detection Anti-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.

	<p><u>Virus Scan Engine Update Capabilities</u></p> <ul style="list-style-type: none"> • 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. • 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. <p><u>Anti-Virus Software Configuration Security</u></p> <ul style="list-style-type: none"> • Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement. • Anti-virus software shall support multiple & customizable definitions of security and rights to various levels of the software configuration settings. <p><u>Anti-Virus Installation Criteria</u></p> <ul style="list-style-type: none"> • Anti-virus software shall be capable of automatic deployment and installation via the following: <ul style="list-style-type: none"> ○ Installation via image – anti-virus software shall be able to be included in the standard workstation 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 deployment (and updates) shall be transparent to end-users. • Anti-virus software shall provide “Wizard-enabled” installation routines to automate and expedite installation. <p><u>Service and Support</u></p> <ul style="list-style-type: none"> • State of Missouri anti-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: <ul style="list-style-type: none"> ○ 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. ○ General advice to end-users on attacks and avoidance measures.
<i>Document Source Reference #</i>	N/A

Standard Organization			
------------------------------	--	--	--

<i>Name</i>	ICSA Labs	<i>Website</i>	www.icsalabs.com
-------------	-----------	----------------	--

<i>Contact Information</i>	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov/
<i>Contact Information</i>	inquiries@nist.gov		
KEYWORDS			
<i>List all Keywords</i>	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, PC		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Conditional Use Restrictions			
<i>Document the Conditional Use Restrictions</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>		
AUDIT TRAIL			
<i>Creation Date</i>	02-06-2003	<i>Date Accepted / Rejected</i>	02-27-2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			