



# Compliance Component

## DEFINITION

<i>Name</i>	Virus Detection and Elimination Criteria for Servers
<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 servers.
<i>Rationale</i>	All servers 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 server trust and security through a set of criteria for the following security services: <ol style="list-style-type: none"> <li>1. Protection to servers and media from computer virus intrusion.</li> <li>2. Detection of computer viruses on an infected server system or media.</li> <li>3. Server recovery from a computer virus infection.</li> </ol>

## 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><b>Virus Detection and Elimination Criteria for Servers</b></p> <p>State of Missouri servers 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 Server Anti-Virus Criteria</u></p> <ul style="list-style-type: none"> <li>• Anti-virus scanner software shall be run on all servers even if the networks perimeter devices are scanning for viruses.</li> <li>• All servers shall be scanned for viruses at least once a day.</li> <li>• Server anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite.</li> <li>• All State of Missouri servers shall execute a virus scan product certified by the ICSA Labs (<a href="http://www.icsalabs.com">http://www.icsalabs.com</a>). ICSA Labs certification requires anti-virus products to detect 100% of all viruses "in the wild" as captured by the WildList Organization</li> </ul>
---	--

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 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

	<p>through a manual or automated process.</p> <ul style="list-style-type: none"> <li>• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures &amp; scan engine techniques (new viruses are discovered daily)</li> <li>• Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.</li> <li>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.</li> </ul> <p><u>Anti-Virus Software Configuration Security</u></p> <ul style="list-style-type: none"> <li>• Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement.</li> <li>• Anti-virus software shall support multiple &amp; customizable definitions of security rights to various levels of the software configuration settings.</li> </ul> <p><u>Anti-Virus Installation Criteria</u></p> <ul style="list-style-type: none"> <li>• Anti-virus software shall be capable of installation on clustered servers.</li> <li>• Anti-virus software shall be capable of automatic deployment and installation via the following: <ul style="list-style-type: none"> <li>○ Installation via image – anti-virus software shall be able to be included in the standard file server images deployed within the enterprise.</li> <li>○ Remote installation – anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.</li> </ul> </li> <li>• Anti-virus software shall provide “Wizard-enabled” installation routines to automate and expedite installation.</li> </ul> <p><u>Service and Support</u></p> <ul style="list-style-type: none"> <li>• Virus protection for servers shall support full virus protection in clustered server environments.</li> <li>• State of Missouri virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.</li> <li>• 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.</li> <li>• Anti-virus vendors shall provide “Virus Catalog Support” including: <ul style="list-style-type: none"> <li>○ A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.</li> <li>○ Downloads or links to disinfection tools.</li> <li>○ A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.</li> <li>○ General advice to end-users on attacks and avoidance measures.</li> </ul> </li> </ul>
<i>Document Source Reference #</i>	N/A

<b>Standard Organization</b>			
------------------------------	--	--	--

<i>Name</i>	ICSA Labs	<i>Website</i>	<a href="http://www.icsalabs.com">www.icsalabs.com</a>
-------------	-----------	----------------	--

<i>Contact Information</i>	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
<b>Government Body</b>			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	<a href="http://csrc.nist.gov/">http://csrc.nist.gov/</a>
<i>Contact Information</i>	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>		
<b>KEYWORDS</b>			
<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, server		
<b>COMPONENT CLASSIFICATION</b>			
<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>		
<b>Rationale for Component Classification</b>			
<i>Document the Rationale for Component Classification</i>			
<b>Conditional Use Restrictions</b>			
<i>Document the Conditional Use Restrictions</i>			
<b>Migration Strategy</b>			
<i>Document the Migration Strategy</i>			
<b>Impact Position Statement</b>			
<i>Document the Position Statement on Impact</i>			
<b>CURRENT STATUS</b>			
<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>		
<b>AUDIT TRAIL</b>			
<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>			