Compliance Component

DEFINITION	
Name	Virus Detection and Elimination Criteria for Anti-Virus Management Tools
Description	To make available to the State of Missouri Enterprise a set of minimum criteria for the selection of Enterprise Anti-Virus Management Tools.
Rationale	All Enterprise Anti-Virus Management Tools within the State of Missouri computer environment must conform to a minimum set of compliance criteria. These criteria should serve as a checklist to help administrators choose the appropriate Anti-Virus Enterprise Management solution for their environment.
Benefits	Integrating all tiers/layers of anti-virus protection software with a good anti-virus software management system helps facilitate the installation, monitoring, and virus update processes to make the security environment flexible and responsive for administrators and as transparent as possible for end-users.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Anti-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 Anti-Virus Management Tools** Keeping anti-virus software up to date is critical. Remembering to keep a single workstation or server up-to-date is not too demanding, but keeping all of the workstations, servers and gateways across a large network up-to-date is a much more difficult task. Anti-virus management tools help administrators with these and other anti-virus automation tasks. Key Anti-Virus Management Tool Criteria include: <u>Enterprise Enforcement of Security Policies</u> • Anti-virus Management tools should offer the capability to centrally configure an anti-virus policy on managed computers. This includes, but is not limited to, enterprise-wide anti-virus polices such as: o Anti-virus engine and signatures updating frequency o The types of files to be scanned

- Scanning schedules
- Heuristic scanning settings

- Management tools should have enforcement features that monitor and enforce the use of anti-virus software across the enterprise, preventing end-users from altering the configuration of the scanner on workstation machines.
- Management tools should provide for the hierarchical grouping of servers and clients for centralized configuration and scanning logs.
- Management tools should allow for remote user monitoring and tracking to fully support policy management of occasionally connected mobile users.
- Management tools should allow for remote scanning initiation on managed computers.

<u>Enterprise distribution of Anti-Virus software and signatures</u>

- Anti-virus management tools should provide rapid, controlled installation across the network and automated updates of all managed machines from a central point of control.
- Management tools must provide the ability to automatically distribute anti-virus packages (anti-virus applications, virus signature files, scan engine updates, etc.) from a local host or via a remote console.
- Such tools must also perform integrity checking of the distributed packages to ensure the package has not been corrupted since it was created for distribution.
- Management tools must offer flexible distribution controls, allowing administrators to schedule automated package distribution at specified times or upon specified events (such as at log-on).

<u>Anti-Virus Management Reporting</u>

- When a virus is detected within the enterprise, anti-virus management tool alerting features should be extensive in order to reach the administrator, whether by network broadcast, fax, E-mail or pager.
- Anti-virus management reports should be customizable to accommodate differences in enterprise networks.
- Anti-virus Management tools should provide graphical, presentation-quality reporting capabilities.
- Anti-virus management reporting should be able to capture data from multiple scan-engines found on managed computers.

<u>Service and Support</u>

- State of Missouri anti-virus management products must be backed by vendors who offer 24 x 7, 365 days a year phone support.
- Anti-virus vendors must 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 must 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 administrators 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*	02-27-03

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