Compliance Component

DEFINITION	
Name	Virus Detection and Elimination Criteria for Wireless Devices
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 Wireless Devices (e.g. PDAs) which connect directly (via a wireless adapter) or connect indirectly (via a cradle) to Missouri's computer networks. All Wireless Devices used within the State of Missouri computer environments that are directly or indirectly connected to enterprise networks or computers 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.
Rationale	When using wireless devices there is a major security gap, as server and workstation anti-virus applications can't protect from a virus being introduced during a sync operation with the wireless device.
Benefits	To significantly improve wireless device trust and security through a set of criteria for the following security services: 1. Protection to workstation computer systems and servers from computer virus intrusion transmitted via wireless devices. 2. Detection and protection computer viruses on an wireless handheld system. 3. Wireless handheld device 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 Wireless Devices** Wireless devices, which connect to State of Missouri systems or networks, shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General Wireless Handheld Anti-Virus Criteria</u> • Wireless anti-virus software shall protect the sync operation and/or the wireless device, even if the workstation and network perimeter

devices are scanning for viruses.

- Wireless handheld anti-virus software shall protect against malicious data as transferred via:
    - Sync operations with a workstation or network
    - Infrared transfer with another handheld device, laptop, or workstation
    - Wireless network or Internet connections
- Wireless virus protection shall cover all major palm top operating systems including:
    - Palm OS
    - Pocket PC
    - Windows CE
    - Symbian EPOC

<u>Virus Detection/Scanning Capabilities</u>

- Wireless device anti-virus software shall be capable of detecting malicious software before it is transferred to workstations or networks.
- 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 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).

<u>Post-Detection Anti-Virus Action Capabilities</u>

- If a virus is discovered, all synchronization between the wireless device and the workstation or network shall be disabled until the destructive code can be removed from the device.
- 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, 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 during synchronization processes. • Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection. Anti-Virus Installation Criteria • Anti-virus software shall be capable of flexible deployment techniques. • 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. 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: o A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them. o Downloads or links to disinfection tools. o 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	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA 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, palm top, palm pilot, handheld, PDA		
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			