# Compliance Component

## DEFINITION

| | |
|---|---|
| *Name* | Virus Detection and Elimination Policies and Best Practices |
| *Description* | To help organizations understand the issues they face when considering the threat from computer viruses and help them through the identification of industry best practices in order to develop an anti-virus policy. |
| *Rationale* | Provides a resource for establishing and tailoring organizational anti-virus policy by raising key issues, listing best practices in virus detection and elimination, and providing suggested security policy guidance. |
| *Benefits* | • Sound anti-virus policies and procedures assist in preventing malicious software from entering the State of Missouri IT environments.<br>• Recommended practices and processes can help prevent the negative effects of viruses. |

## 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 Policy Guidelines**<br>1. **Every State of Missouri Agency and/or organization shall have a formal Virus Detection Policy.**<br>• Developing an effective virus protection policy is a crucial component of every agency's security plan. Such a policy shall accomplish two goals:<br>a. Detail the IT department's procedures for preventing and managing virus outbreaks.<br>b. Educate end-users about their roles and responsibilities in preventing virus outbreaks.<br>**2. All State of Missouri computer systems shall have MAEA approved anti-virus software installed and scheduled to run at regular intervals.**<br>• This applies to all State of Missouri computer systems. This includes, but is not limited to, workstations, laptops, servers, gateways, and wireless devices. |

- In addition, the anti-virus software and the virus pattern files shall be kept up-to-date.

3. **File Transfers, Downloads and Attachments**
    - Any file transferred into and within the State of Missouri computer environments shall be scanned for virus infection prior to execution or use.

4. **Training shall take place to ensure that all computer users know and understand safe anti-virus computing practices.**
    - Virus education and training shall include information on the following:
        - Before installation, the source of the software shall be known.
        - Use of write-protected program installation media only.
        - Performing frequent backups on data files.
        - Use of virus detection software.
        - Scanning for viruses on files that are downloaded from the Internet or any other outside source.
        - Scanning for viruses on all media brought from any outside source.
        - A requirement that end-users first contact their Information Technology Department before directly adding any software to the system.

5. **Virus incident management procedures shall contain:**
    - Verification of a virus threat and rule out the possibility of a hoax, before notification of the threat is broadcast.
    - The identity of personnel responsible for mitigation of virus threats.
    - Internal escalation procedures and severity levels.
    - Processes to identify, contain, eradicate, and recover from virus events.
    - An up-to-date contact list of the organization’s anti-virus vendors.
    - Reporting of all virus outbreaks that have extended beyond a single computer within the State of Missouri enterprise (incident response link).

**Virus Detection and Elimination Best Practices**

1. **Implement a layered defense strategy for virus protection.**
    - The most effective way to ensure that the State of Missouri computing environment remains virus-free is to monitor all entryways for viruses using multiple scan engines at different tiers within the network. Entryways/tiers include:
        - Internet gateways and Internet Servers
        - Groupware and E-Mail Servers
        - LAN based servers (such as File and Print Servers)
        - Workstations
        - Wireless devices
    - A combination of multiple scan engines can reduce single points of failure and create a unified anti-virus framework.

2. **Encourage distributed responsibility / Establish an virus response team**
    - Similar to an emergency response team or other cross-disciplinary group within an organization, an virus response team can be assembled, then trained and empowered to deal calmly, effectively and professionally with any virus incident.
    - When an incident does occur, specific people are already selected to immediately tackle cleanup.
    - Providing team members with specific roles and authority sends a message to all employees that virus protection is important and that it involves more than IT staff.

3. **Periodically review the anti-virus policy**
    - An annual review is necessary to reflect changing conditions and serves to reinforce important anti-virus issues that may not have been discussed for some time.

4. **Attachments.**
    - Assume that ANY attachment you receive may be potentially infected, even if you know the author.
    - Since many viruses originate from an infected computer and its address book, viruses will most likely come from family, friends, or business associates.
    - When processing E-mail, only open messages and/or attachments that you are expecting. Avoid opening any E-mail attachment if it appears to be of a suspicious nature.
    - Virus writers use social engineering tricks to tempt individuals into "taking the bait" on attachments, so always be careful.

5. **Anti-virus files (patches, signatures, and engines) need to be updated continuously either through a manual or automated process.**
    - End-users are far more likely to get a brand new virus in current circulation or outbreak mode, than an older virus that has been contained and is no longer active.
    - Laptop PC users shall connect their laptop to the network and get the latest anti-virus updates installed before taking the laptop out of the office.

6. **Periodic System Checks**
    - All equipment and software within an organization’s computer environment shall be scanned at predefined time intervals to ensure that the environment is free of any virus corruption.

7. **System Integrity Checking**
    - All of an organization’s personal computers and servers shall run integrity checking software. This software detects changes in configuration files, system software files, application software files and other systems resources.
    - Integrity checking software shall be continuously enabled or run daily.

| | | | |
|---|---|---|---|
| | **8. Write permissions to software**<br>• With the exception of software that shall modify itself in order to execute, write permissions to software shall be carefully controlled such that an error will be generated if a computer virus tries to modify the software.<br>**9. Stay Informed**<br>• Major new virus outbreaks will surface frequently. Anti-virus vendors shall provide formal alerts.<br>• IT personnel shall also remain pro-active about virus developments to avoid problems associated with major attacks. | | |
| *Document Source Reference #* | N/A | | |
| **Standard Organization** | | | |
| *Name* | TruSecure Corporation | *Website* | www.trusecure.com |
| *Contact Information* | 1-888-396-8348 (info@trusecure.com)<br>Anti-Virus Policy Guide Version 3.6.0 [AVPG360.pdf] | | |
| *Name* | TechRepublic | *Website* | www.techrepublic.com |
| *Contact Information* | http://www.techrepublic.com/contact.jhtml<br>Virus Protection Policy [virus_protection_policy.pdf] | | |
| **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 detection capability; malicious code; virus products; virus reporting; anti-virus vendors; anti-virus engine; hoax; | | |
| **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* | 06-28-2006 |
| *Reason for Update* | Update link | | |