RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

IT Office for Undergraduate Academic Affairs and Student Affairs

IT SERVICES POLICY

Policy Name: Anti-virus and Malware Policy

Originally issued: 07.07.08

Revisions: 11.07.13

Policy at a Glance

- *All devices supported by UAA/SA IT Services must have current, ITS approved anti-virus software installed that is directly managed and updated by ITS*
- *Users are responsible to inform IT staff immediately if they suspect an infection or compromise*
- *If a device appears that it is infected or compromised, it will be disabled or taken offline immediately until it is confirmed to be malware free and the source of the infection will be determined, mitigated, and escalated as necessary*
- *If a device becomes infected and the source is user behavior, the user will be made aware of how to avoid infection or compromise. If the behavior is not changed, supervisory action will be taken*

1. **Policy Statement**
   This policy outlines anti-virus requirements and related administrative procedures for the divisions of Undergraduate Academic Affairs (UAA) and Student Affairs (SA).

2. **Reason for Policy**
   It is the goal of this anti-virus policy to:
   - Protect the data and integrity of all UAA/SA ITS resources
   - Minimize downtime due to malware infection
   - Set expectations for users
   - Set communication parameters
   - Set expectations for enforcement

3. **Who Should Read This Policy**
   All users of networks and systems managed by UAA/SA IT Services.

4. **Related Documents**
   [Under revision]

5. **Contacts**
   http://its.rutgers.edu/help-desk

SCOPE

This policy applies to all computing and network-related resources of the divisions of UAA and SA, whether located on campus, or at remote locations and facilities. These resources include but are not limited to:

- Desktops, laptops, tablets and servers; the software running on these devices; and vendor supplied software services and contracting
- Peripheral equipment (e.g. printers, scanners, network copiers, anything that plugs into a computer, etc.)
- Cabling or connectivity-related devices (switches, hubs, firewalls, etc.)

Note: Departments not covered by this policy are departments supported by the Old Queens technical support team, Recreation Services, and Dining Services.

POLICY

Standards

All UAA/SA IT Services computers and computers residing on networks where UAA/SA IT Services is the Network Liaison to OIT (Telecommunications Division) must have Rutgers University's standard, supported anti-virus software installed and scheduled to run full malware scans (at minimum, weekly) and definition updates (at minimum, daily) at regular intervals

UAA/SA IT Services

- Windows and Macintosh OS-based systems must have a minimum Symantec Endpoint Protection Software installed
- Devices with operating systems other than those based on Microsoft or Macintosh products are excepted from this anti-virus installation requirement at the current time
- The anti-virus software and the virus pattern files must be kept up-to-date
- Malware-infected computers must be removed from the network until they are verified as virus-free
- For groups that are not directly managed by UAA/SA IT Services, system managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. RADS (http://rads.rutgers.edu) or departmentally managed Symantec Endpoint Protection antivirus software must be used.
- Any activities with the intention to create and/or distribute malicious programs into Rutgers University's networks (e.g., viruses, worms, Trojan horses, malware, e-mail bombs, etc.) are prohibited, in accordance with the Rutgers University Acceptable Use Policy for Computing and Information Technology Resources

Anti-virus installation requirements

- Managed domain-based workstations and servers use Symantec Endpoint Protection Software client managed by a UAA/SA ITS
    - Defined as any workstation within the RC and ITS active directory domains or "bound" Macintosh OS-based devices or primary systems administrator is a full-time staff member from UAA/SA ITS and not in the domains listed above
- Unmanaged systems
    - Not meeting criteria above, must still have RADS or preferably SEP installed

Responsibility

It is the responsibility of the systems administrators, the users, and their supervisors to avoid contact with malware and behaviors that have the potential for introducing malware into the computing environment

- System administrators and IT staff
    - Must install current anti-virus and anti-virus on all workstations and servers as well as provide a mechanism for regular updates
- Users
    - While it is difficult to avoid or understand the nature of all threats, the user must avoid exposure to threats wherever possible by:
        - Reading alerts distributed by UAA/SA ITS
        - Reporting suspicious computer behavior to the UAA/SA IT Services Helpdesk
        - Avoid repeating behavior that has previously resulted in system infection or attempted infection
        - Providing accurate information if infected to UAA/SA IT Services personnel
- Supervisors
    - Assist users and UAA/SA IT Services personnel in communicating procedures and policies
    - Take supervisory action when notified of a user's behavior resulting in exposure to malware to prevent repeated exposure
    - Ensure compliance with UAA/SA and Rutgers University policies and procedures

Communication

- Communication is an essential element in malware prevention, detection and eradication
- UAA/SA IT Services staff are required to inform users and the Director of ITS (Assistant Director in the absence of the Director) immediately of:
    - malware threats with potential for exposure
    - active infections
    - behavior leading to malware exposure

- Users and supervisors are required to inform the ITS Helpdesk immediately of:
  - suspicious computer activity including but not limited to
  - error messages
  - large amounts of pop-up advertisements
  - system failure
  - anti-virus alert messages
  - potential or known malware exposure
  - home computer infection (shared USB drives, etc.)
  - alert messages from shared disks, drives, or email

Enforcement

- If any system is exhibiting behavior consistent with a malware infection:
  - The system will be temporarily taken off the network until an on-site inspection and scan can be made
  - The system will be referred to Rutgers University authorities if any potential data compromise has taken place
- Managed workstations and servers
  - Depending on the level of the potential infection, a remote scan and review will be made
  - If the system is found to have residual infection or potential for residual infection, the system will be re-imaged
  - If a Trojan horse or backdoor was installed, the system will be imaged for forensic evaluation prior to re-installation
  - Once the attack vector is identified
    - Reinstallation will take place
    - The threat must be mitigated to all remaining systems
- Unmanaged workstations and servers residing on UAA/SA ITS networks
  - The system will remain off the network until the systems administrator of the "unmanaged system":
    - is notified
    - completely identifies the nature of the infection and that is consistent with observed and/or reported behavior
    - reports the system as cleaned and/or rebuilt, patched, and the attack vector has been mitigated
    - If no systems administrator is identified, one must be determined to prevent future problems from occurring

Repeated infections

- UAA/SA IT Services will attempt to work with users to educate them about behavior leading to infection. The third notification or particularly egregious behavior will result in supervisory notification
- Users unwilling to modify behavior leading to infection may face system limitations on the network and the user's supervisor will be notified
- Users unwilling to modify behavior leading to infection outside of the UAA/SA IT Services domain will be unable to utilize the network infrastructure