University Community (faculty, staff and students) and Authorized Users of University’s IT Resources (e.g., consultants, vendors, etc.)

PROCEDURE STATEMENT (R)
This procedure is in accordance with administrative and technical requirements set forth in State and Federal Law. All University-owned computing hosts that are subject to virus infection and are connected to the University network must have anti-virus software running, and anti-virus definition updates applied to them within 24 hours of their release. A list of approved anti-virus software systems for various operating systems that need protection is available at security.fiu.edu. Networked devices that are subject to virus infection, and are unable to use anti-virus software, must be protected from malicious network traffic via host or network-based firewalls, and must be reported to the Information Technology Security Office ("ITSO").

All computers owned by the University, regardless of which operating system they use, must have current and appropriate operating system and applications software patches applied. Application of current and appropriate operating system and applications software patches may be accomplished by (1) University Technology Services, or (2) by the department/unit housing the equipment with the approval of the ITSO.

Exceptions to this requirement may be appropriate for patches that compromise the usability of an operating system or application when installed, or for patches for which the installation is prohibited by regulation. All exceptions must be documented, reviewed, and approved by the ITSO.

Circumstances when a computer not owned by the University is connected to the FIU Network, the owner must have (1) approved anti-virus software installed, maintained, and updated on the computer and (2) must have current operating system and applications software patches applied to the computer.

Any computer that is compromised, and is connected to the FIU Network will be blocked from access to the network until it is determined by the ITSO that the compromised computer no longer poses a threat to the network.

REASON FOR PROCEDURE (O*)
The University is subject to federal and state laws that require that it have in place administrative and technical standards to safeguard the confidentiality, integrity and availability of the data it creates and maintains. The University must protect computer systems on the FIU Network from being compromised by the introduction of viruses, worms, or other malicious programs. Computers are most often made vulnerable to compromise as the result of: (1) not having effective anti-virus software installed, and/or (2) not applying necessary system updates (software and hardware revisions and patches). Not only could neglect in this area affect an individual user, but also, as a result of a system being compromised, it could affect other users who use FIU Information Technology Resources (ITR), and networked users external to the University.

DEFINITIONS (R)
Anti-virus definition files - Update files periodically provided by the anti-virus software vendor that ensure that the anti-virus software can identify and contain all currently known computer worms or viruses.

Audit - System Security Scan - A tool that scans systems for vulnerabilities and provides reports of findings.

Compromised System - A computer or server whose operating system has been altered by external means so as to perform malicious, disruptive, or unexpected action(s), (virus propagation, sending of junk e-mail, etc.).

FIU Information Technology Resources (ITR) - Computing/networking equipment and technology-related services provided by the University.
FIU Network - The University’s intercampus network, FIUnet, including all connected sub-networks.

ITSO - FIU Information Technology Security Office.

Patch/Update - An operating system or applications software update that is provided by the operating system or application vendor and labeled as a security vulnerability patch.

Threat - Any condition that could affect confidentiality, availability, and integrity of FIU’s information technology resources.

UTS - University Technology Services.

RESPONSIBILITIES (O)

UTS will control the distribution of Anti-Virus definition files and Operating System updates unless permission for an exemption has been granted, in writing, by the ITSO and the Chief Information Officer.

Managers and Administrators of Information Systems:
- Enforce system and anti-virus update requirements.
- Evaluate updates and supply the necessary means within the FIU network for users to obtain the updates.
- Stay current with and aware of all recommended updates.
- Notify UTS Support Center if there is a conflict distributing an update to campus users.

All employees and students and owners of non-FIU computers connected to, or using FIU information technology resources:
- Install, maintain and update FIU approved anti-virus software and system updates in a timely manner.
- Contact the UTS Support Center if you have questions or concerns about the status of your updates.
  See Guidelines here: (http://security.fiu.edu/securing_PCs.htm)

IT Security Office:

The IT Security Office has the responsibility to evaluate the seriousness and immediacy of any threat to campus information system resources or to the Internet and to take action to mitigate that threat. Action that is taken will be responsible and prudent. Action taken will be based on the risk associated with the threat and also the potential negative impact to the University’s mission that may be caused by making the offending computer(s) inaccessible. Please refer to FIU IT Security Blocking Procedures, which are available on the ITSO website. The ITSO is also responsible for the following:

- Review procedures for providing system and anti-virus updates.
- Perform random audits on systems to verify system and anti-virus updates.
- Evaluate and mitigate threats to ITR or the Internet.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)
Division of Information Technology
Florida International University

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)
FIU IT Security Office
Biscayne Bay Campus, LIB 328
3000 N.E. 151st Street
Miami, Florida 33181
Telephone Number: (305) 919-4299

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at http://policies.fiu.edu/.

For any questions or comments, the “Document Details” view for this procedure online provides complete contact information.

FORMS/ONLINE PROCESSES (O)

FIU IT Security Blocking Procedures

Link(s) to the above referenced Forms available in the "Document Details" Section of the online version of this policy document.

R*=Required  O*=Optional