FIU FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

IT Security: System and Application Management # 1930.023

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	May 20, 2024	Division of Information Technology/IT Security Office

POLICY STATEMENT

This policy 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 an up-to-date endpoint protection software installed and running. A list of approved endpoint protection software 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 endpoint protection 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.

SCOPE

This policy applies to all faculty, staff, and students and authorized third party affiliates (consultants, vendors, persons of interest)

REASON FOR POLICY

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 endpoint protection 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

TERM	DEFINITIONS
Audit-System Security Scan	A tool that scans systems for vulnerabilities and provides reports of findings.
Compromised System	A computer or system whose operating system has been altered by external means so as to perform malicious, disruptive, or unexpected actions(s), (virus propagation, sending of junk e-mail, etc.)
FIU Information Technology Resources (IRT)	Computing/networking equipment and technology-related services provided by the University.
FIU Network	The University's Intercampus network. FIUnet, including all connected sub-networks.
Threat	Any condition that could affect confidentiality, availability, and integrity of FIU's information technology resources.
Patch/Update	An operation system or applications software update this provided by the operating system or application vendor and labeled as a security vulnerability patch

ROLES AND RESPONSIBILITIES

Division of Information Technology Services will control the distribution of endpoint protection software 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:

- Endpoint protection software must be installed on all endpoints.
- Enforce system and endpoint protection updates.
- Managed endpoints should have SCCM configured.
- 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.
- Review vulnerability reports and reply to the IT Security Office regarding these reports.
- Mitigate identified vulnerabilities in a timely manner.
- Hard Drives should be encrypted with whole disk encryption.
- Notify Division of Information Technology 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 threat prevention software and system updates in a timely manner.
- Local Firewall should be enabled.
- Contact the Division of Information Technology Support Center if you have questions or concerns about the status of your updates.
- See Guidelines here: (http://security.fiu.edu)

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.

The ITSO is also responsible for the following:

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

RELATED RESOURCES

Security Office Website https://security.fiu.edu

Software Center Updates to Machines on Active Directory: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010363

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 St, PC534a
Miami, FL 33199
305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: October 2007
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): June 9, 2021; May 20, 2024 (formerly 1930.020c procedure converted into policy)