FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Responsibilities for FIU Network and/or System Administrators #1910.005

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
April 6, 2009	May 21, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

University academic or administrative units that plan to operate or maintain unit specific networks and/or systems must first obtain the approval of the Vice President with oversight over the area, if administrative, the Provost or his designee, if academic, and the Vice President and Chief Information Officer. This approval process shall ensure that unit specific network and systems are implemented and maintained in accordance with all applicable federal and state laws and University rules, regulations, policies and procedures including those applicable in the area of purchasing, information technology resources and security, among others.

Network or System Administrators who report to a department, school or administrative head must keep the Chief Information Officer informed of all appropriate matters involving the use of information technology resources at the University.

It is required that the Network or System administrator follow the guidelines of their administrative unit as well as all pertinent Florida International University rules, regulations, policies, procedures, licensing agreements, and federal and state laws.

SCOPE

This Policy applies to all Network, systems, application administrators or any other user which is responsible for administering information systems, devices, and/or applications at FIU, including third party affiliates (consultants, vendors, Person of Interest) with administrative access and/or responsibilities.

REASON FOR POLICY

To outline the approval process for an academic or administrative unit to implement a unit specific network or system, and to provide guidelines for Network and System Administrators to understand their responsibilities in ensuring that unit specific guidelines are in accordance with the policies and procedures of the University for the purchase, implementation, maintenance, use and ultimate disposition of, information technology resources.

DEFINITIONS	
TERM	**DEFINITIONS**
Information Technology Administrators Committee ("ITA Committee")	Committee comprised of all Florida International University Network and/or Systems Administrators who have principal responsibility over a university network or system.
Network and/or Systems Administrator	An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only regular full-time or part-time employees of the University and/or third-party vendors who are specifically approved by the Division of IT may function as system/network administrators. Webmasters, developers, application admins, and systems admins, shall be considered Network/System Administrators for purposes of this policy. System/Network Administrators may employ students to assist them in systems administration only under the direct technical supervision of a technically competent System/Network Administrator; such students are covered by this policy.

ROLES AND RESPONSIBILITIES

Network/System Administrators shall ensure that the systems comply with applicable University policies, software licensing agreements, and state and federal laws.

Network/System Administrators shall become members of the ITA Committee's listserv and Team's channel so that they can receive regular and special reminders, announcements and alerts sent out by the VP and CIO of the Division of IT or his designee.

Among their other responsibilities, the Network/Systems Administrator should use reasonable efforts to:

- Implement and maintain an IT Asset Management system that can:
  - Inventory and keep control of hardware assets
  - Inventory and keep control of software assets
  - Follow the university's documented media sanitation process
- Respond and leverage the university's Endpoint Server Management by:
  - Reviewing and remediating vulnerably report findings
  - Reviewing weekly reports
  - Making sure systems are patched and updated
  - Following up Cybersecurity's Threat Prevention reports
  - Controlling the use of Administrative Privileges on machines in their departments.

    - Hardening the configuration for hardware and software on mobile devices laptops, workstations, and servers.
- Implement and maintain a Business Continuity and Disaster Recovery which includes a:
    - Business Impact Analysis
    - Risk Assessment
    - Continuity of Operations (COOP) Plan
    - DR testing and documentation
- Maintain a reasonable preparedness for Incident Response situations by:
    - Being familiar with the Enterprise Incident Response Plan
    - Having an operational Incident Response Process
    - Making sure users are aware of how to report incidents
- Maintain departmental standards by:
    - Creating Standard operating procedures for your business units
    - Documenting routine operations and transfers of responsibility
- Keep adequate Identity Access Management by:
    - Enabling Audit Logs; Also, collecting, storing, and monitoring them on a routine basis.
    - Uniquely Identifying user accounts
    - Using CAS/Login page for web logins

Network/System Administrators, when requested, are expected to cooperate fully with the IT Security Office in any investigation, identification, and resolution of system/network incidents.

The Network/Systems Administrator shall maintain and make readily available to the Division of IT all documentation of any and all devices within their unit that will connect to the University's network. The report must include the following information:

- Manufacturer, model and serial number.
- Operating System and revision number.
- MAC address of all network interface cards within their unit, and as appropriate any permanent Layer 3 network address.
- Computer's host name(s) and primary user's information.
- Physical location of the equipment.
- Network/System administrator's name and phone numbers (office and after-hours).
- System's primary functions (e.g., web services, file server, mail server, personal computer, etc.)
- Disaster Recovery Plan.

It is the responsibility of each academic and administrative unit within the University to define a hierarchy with respect to computer administration. As part of this process, the Network/System Administrator(s) for each academic or administrative unit or subdivision shall be identified. Units should clearly define roles with respect to systems administrator functions, technical data, network traffic, and system files; supervision of Network/System Administrators; and clearly specified authorizations required for review of such files, data or

communications. In addition to the responsibilities outlined above, Network/System Administrators who have responsibility over information systems, servers, workstations, and devices connected to the FIU network will use reasonable efforts to:

- Respond to all requests for support, information, problem determination and problem resolution.
- Supply the Division of IT with contacts and contact information on primary, secondary, and tertiary contacts if it differs from network/system administrator contact information. Contact information should include contact instructions for after hours and weekends.
- Provide appropriate, industry-standard virus screening and filtering services for incoming and outgoing email.
- Maintain a comprehensive electronic directory of e-mail addresses.
- Configure and maintain the application software in a manner to optimize security and respond to ongoing security threats including, but not limited to, the strength of account passwords for subscribers.
- Maintain information systems, devices, servers, workstations, and applications patched and updated.
- Report any suspicious activity, compromise, breach etc. to the Information Security Office.

RELATED RESOURCES

https://security.fiu.edu
Asset Management: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011571
FIU Ready (COOP): https://dem.fiu.edu/resources/fiu-ready/index.html
FIU Security Resources: https://security.fiu.edu/security_resources
FIU Incident Response Plan: https://policies.fiu.edu/policy/862

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 ST, PC534
Miami, FL 33199
Security@fiu.edu
305-348-1366
https://security.fiu.edu

HISTORY

Initial Effective Date: April 6, 2009
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): May 21, 2021