University Community (faculty, staff and students)

**SUBJECT (R*)**
RESPONSIBILITIES FOR FIU NETWORK AND/OR SYSTEM ADMINISTRATORS

<table>
<thead>
<tr>
<th>EFFECTIVE DATE (R*)</th>
<th>POLICY NUMBER (O*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 6, 2009</td>
<td>1910.005</td>
</tr>
</tbody>
</table>

**POLICY STATEMENT (R*)**

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.

**REASON FOR POLICY (O*)**

To outline the approval process in order for an academic or administrative unit to implement a unit specific network or system, and to provide guidelines in order 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 (R*)**

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.

Technical Webmasters 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.

**RESPONSIBILITIES (O*)**

Network/System Administrators must attend regularly scheduled meetings of the ITA Committee, as well as any special meetings that may be called by the VP and CIO of the Division of IT in order to maintain close working relationships and openness in day-to-day communications.

Network/System Administrators must report to the VP and CIO of the Division of IT on a quarterly basis regarding the progress and status of any systems implementation and changes to the IT environment.
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 list serve 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:

- Participate in IT Security Training for Network/Systems Administrator and attend regular meetings as determined by the Division of IT.
- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.
- Treat information stored by the system’s users in an appropriate manner, taking necessary precautions to protect the security of a system or network and the privacy and confidentiality of the information contained therein.
- Promulgate information about specific policies and procedures that govern access to, and use of, the system and services provided to the users.
- Promptly inform the IT Security Office of any computing incidents which clearly compromise system or network integrity, including but not limited to:
  - Notification by outside institutions or individuals of any incident.
  - Data loss or theft.
  - Inappropriate systems or information access or use.
  - Any other breach or violation of IT policies of which they become aware.

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 attach 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 an e-mail server 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.
### RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology  
Florida International University

### RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

Vice President and Chief Information Officer  
Florida International University  
11200 S.W. Eighth Street, PC 507  
Miami, Florida  33199  
Telephone Number: (305) 348-2738

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/](http://policies.fiu.edu/).

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

*R = Required  *O = Optional