



| | | |
|--|--|---|
| SUBJECT: ACCEPTABLE USE OF TECHNOLOGY RESOURCES | Effective Date: 5-31-11 Amended: 8-21-17; 10-23-18 | Policy Number: 12.2 |
| | Supersedes: IRM Techpolicy V-D, VI-B,D,K | Page Of 1 3 |
| | Responsible Authority: Associate Provost and Chief Information Officer | |

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all users of University technology resources, including without limitation telecommunications, networks, email, computing resources, and instructional technology resources.

POLICY STATEMENT:

I. POLICY

- A. *Laws and regulations:* All users are responsible for adhering to all applicable federal, state, and local laws and regulations and all University regulations and policies, specifically including without limitation the University’s sexual harassment regulations and policies, those pertaining to the privacy of student records (FERPA), and the Digital Millennium Copyright Act (DMCA).
- B. *Copyright:* All users are responsible for respecting the copyrights of others and must refrain from unauthorized distribution, downloading and use of copyrighted works.
- C. *Campus-provided system services:* Users shall not intentionally set up services that interfere with University provided services without the express written permission of the Office of Information Technology.
- D. *Unauthorized access:* Users shall not access resources, files, and networks to which they were not granted access, or in excess of their approved access.
- E. *Intentional Interference:* Users shall not intentionally interfere with communications or systems in such a way as to impair their ability to function or provide services as expected.

- F. *Capturing or monitoring communications*: Users shall not capture or monitor any communications sent by, or destined for systems that are not within their responsibility without the written permission of the Information Security Officer and the Chief Information Officer.
- G. *Vulnerability Testing*: Users shall not intentionally scan for or exploit vulnerabilities on systems that are not under their responsibility without the written permission of the Information Security Officer and the Chief Information Officer.
- H. *Forged communications*: Users shall not modify their communications in order to make it appear as if the communications came from another source such as through the use of anonymizing services.
- I. *FAU-provided Accounts*: Users are not permitted to share their FAU NetID password with any other person. FAU NetID passwords are treated as secrets that should only be known by the individual to which the NetID was assigned. Users are responsible for their own user accounts.
- J. *Shared Accounts/Generic Accounts*: The University does not provide shared or generic accounts due to accountability requirements.
- K. *Network Traffic*: Users are responsible for the traffic originating from their computing devices including, but not limited to, file sharing and abusive or malicious activity.
- L. *Security*: Users are responsible for ensuring the security of their computing devices. This includes ensuring that the computing device is kept up to date with vendor supplied security patches and running personal firewall and antivirus software where applicable. Devices and software for which a vendor no longer provides security patches may not be used on FAU networks or on a system connected to FAU networks unless a specific written exemption is granted by the Information Security Officer.
- M. *Personal/Financial Use*: University technology resources may not be used for personal financial gain unless approved by the President or Provost. De minimus non-commercial personal use is permitted so long as such use does not violate any other provision of this policy or interfere with job responsibilities. Email blasts for personal purposes are not permitted.
- N. *Email Signatures*: Email signatures for University business communications may only include University-related contact information. Only current titles and positions may be listed. Email signatures may not include personal statements, messages, images or links, including, but not limited to, spiritual, political, philosophical, religious, poetic, or other personal statements, messages, images, or links.
- O. *Circumvention of Security Controls*: Users shall not circumvent information security controls in place at the University without the express written permission of the Information Security Officer and the Chief Information Officer.
- P. *Remote Access to Devices on the FAU Network*: Users may only access devices and software connected to FAU networks through methods approved in writing by the Information Security Officer or provided directly through the Information Security Office including, but not limited to, firewall controls or FAU's Virtual Private Network (VPN).

- Q. *Rogue Networks*: Computer networks that are connected to FAU networks must be approved by the Director of Communication Infrastructure. Computer networks include, but are not limited to, Wireless Access Points, Network Routers, Network Switches, Hardware Firewalls, Proxy and Network Filtering devices, and site-to-site Virtual Private Networks.
- R. *Automated phone calls or sending of text messages*: Users may not utilize technology resources to initiate automated phone calls (robo-calls) or initiate the automatic sending of text messages for the purposes of marketing or recruitment without explicit written approval from the called/texted party.

II. SANCTIONS

Violations of the policies and laws described herein by an employee or student are grounds for disciplinary action up to and including termination or expulsion in accordance with applicable University and the Florida Board of Governors regulations and/or collective bargaining agreements. Such disciplinary actions may also include reprimand or suspension. Violations of these policies and laws by any users are grounds for terminating their use of University technology resources and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal charges, as appropriate. The filing of criminal charges similarly does not preclude action by the University.

III. RELATED INFORMATION

Additional guidance concerning general employee and student conduct can be found in [Regulation 4.007 \(Student Code of Conduct\)](#), the [Employee Handbook](#), the [Faculty Handbook](#), and [University Policy 1.9 \(Fraud\)](#).

IV. INITIATING AUTHORITY: Associate Provost and Chief Information Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 12.2

Initiating Authority
Signature: _____ Date: _____
Name: Jason Ball

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: Elizabeth F. Rubin

President
Signature: _____ Date: _____
Name: Dr. John Kelly

Executed signature pages are available in the Office of the General Counsel