FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

***University Staff (non-bargaining unit faculty and employees), University Students and Authorized Users of University's IT Resources (e.g., consultants, vendors, etc.)***

| SUBJECT (R*) | EFFECTIVE DATE (R*) | POLICY NUMBER (O*) |
|---|---|---|
| INFORMATION TECHNOLOGY SECURITY | July 2005 | 1930.020 |

## POLICY STATEMENT (R*)

*General Responsibility*

Each member of the University community shall adhere to all federal, state and local laws and FIU rules, regulations and policies, as the same may be amended from time to time, pertaining to the security and protection of electronic information resources that he/she uses, and/or over which he/she has access or control.

Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Contractors and participants in any activities outsourced to non-FIU entities must comply with the same security requirements.

*Protecting FIU's resources is a critical part of its mission.*

As part of Florida International University's mission (http://academic.fiu.edu/docs/provost_mission.htm) we strive to keep our resources safe and secure. In order to fulfill the mission of teaching, research and public service, the University is committed to providing a secure computing and networking environment that assures the integrity, availability, and confidentiality of information and information resources.

*Enforcement*

Persons who fail to adhere to this Policy may be subject to penalties as provided by law and/ or disciplinary action, including dismissal or expulsion. Violations will be handled through the University disciplinary policies applicable to employees and students. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Unauthorized or fraudulent use of University computing or telecommunications resources can also result in felony prosecution as provided for in the Federal and State of Florida Statutes.

*Compliance*

I have read and I understand the above FIU General IT Security Policy and will adhere to all applicable laws, rules, regulations and policies pertaining to the security and protection of the University's electronic information resources.

## REASON FOR POLICY (O*)

To provide guidelines for information technology security.

## RELATED INFORMATION (O*)

*Laws, Rules and Regulations Impacting the Use of Florida International University Information Technology Resources*

*Addressing Privacy and Security Requirements*

This is a representative list of the federal and State of Florida laws, rules and regulations that Florida International University, its

faculty, staff and students must follow in their use of the University's information technology resources. This list is not comprehensive, but is intended to assist the reader to develop a basic understanding of the legal framework applicable to the activities of FIU, its faculty, staff and students in the information technology environment.

Federal Laws:

Child Pornography Prevention Act of 1996, 18 U.S.C. §§ 2251 et seq.
Copyright Laws, 17 U.S.C. §§ 101 et seq.
Credit Card Fraud, 18 U.S.C. § 1029
Criminal Infringement of a Copyright, 18 U.S.C. § 2319
Digital Millennium Copyright Act, 17 U.S.C. §§ 1201 et seq.
Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-39
Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22 ("The Wiretap Act")
Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99 ("FERPA" also known as the "Buckley Amendment")
Fraud and related activity in connection with computers, 18 U.S.C. § 1030 et seq.
Health Insurance Portability and Accountability Act, Administrative Simplification Provisions, 42 U.S.C. § 1320d, et seq. ("HIPAA")
HIPAA Privacy Rule, 45 C.F.R. Part 160; 45 C.F.R. Part 164, Subparts A and E
HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C
Homeland Security Act of 2002, Pub. L. 107-296, 116 Sat. 2135 (HR 2002)
Unlawful Access to Stored Communications, 18 U.S.C. §§ 2701 et seq.
USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272

Florida Laws:

Computer Crimes Act, Fla. Stat. §§ 815.01 et seq., §§ 775.082-084
Computer Pornography and Child Exploitation Prevention Act of 1986, Fla. Stat. §§ 847.0135 et seq.
Florida Public Records Act, Fla. Stat. Chapter 119

FIU IT Policies:

FIU Code of Computing Practice
FIUnet Acceptable Use Policy
IT Security Policies

**RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)**

Division of Information Technology
Florida International University

**RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)**

IT Security Office
Division of Information Technology
Florida International University
11200 SW 8 Street, PC534A
Miami, FL 33181
Telephone Number: (305) 348-3712

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 policy online provides complete contact information.

**FORMS/ONLINE PROCESSES (O*)**

FIU Code of Computing Practice
FIUnet Acceptable Use Policy
IT Security Policies

Employees who are bound by this policy, students and authorized users of the University's IT resources will be asked to confirm their understanding of, and agreement to abide by this policy via an online process:

*Confirmation*

Please enter your Panther ID and Username for confirmation that you have read and understood the FIU Information Technology Security Policy. Failure to do so may result in the loss of access to FIU Information Technology Resources.

Panther ID _____
Username _____

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

***R = Required  *O = Optional**