



**Information Technology Security (SEIU) # 1760.127**

<b>INITIAL EFFECTIVE DATE:</b>	<b>LAST REVISION DATE:</b>	<b>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT</b>
May 8, 2006	May 17, 2024	Division of Information Technology

**POLICY STATEMENT**

As part of Florida International University’s mission, 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.

**SCOPE**

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.

**REASON FOR POLICY**

At Florida International University, as custodians of sensitive information, it is incumbent upon the university to safeguard the integrity, availability, and confidentiality of our resources. This policy is driven by our commitment to uphold the highest standards of academic and operational integrity.

<b>DEFINITIONS</b>	
<b>TERM</b>	<b>DEFINITIONS</b>
Information Technology Resources	Refers to any technology-related assets, including but not limited to networks, computers, software, and data, utilized by FIU for academic, administrative, or operational purposes.
Integrity	The assurance that information and information resources are accurate, reliable, and protected against unauthorized alteration or tampering.



Availability	Ensuring that information and resources are accessible and usable by authorized users whenever needed, without interruption or delay.
Confidentiality	The protection of sensitive information from unauthorized access, disclosure, or use, maintaining its privacy and restricting access only to authorized individuals or entities.
General Responsibility	Each member of the university community's obligation to comply with all applicable laws, regulations, and institutional policies regarding the security and protection of electronic information resources to which they have access.
Threats	Any potential risks or vulnerabilities that may compromise the physical or logical integrity of information technology resources, including unauthorized intrusions, malicious misuse, or inadvertent compromise.
Contractors	Individuals or entities engaged by FIU to provide services or that participate in activities outsourced to non-FIU entities, who are required to adhere to the same security requirements as specified in this policy.
Enforcement	The actions taken by FIU to ensure compliance with this policy, including penalties as provided by law and disciplinary measures, such as dismissal or expulsion, for individuals who fail to adhere to the policy.

**ROLES AND RESPONSIBILITIES**

Each member of the University community is responsible for adhering 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.

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.



## RELATED RESOURCES

### 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 Stat. 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

### Helpful Links:

[Official Web site for the U.S. Patent and Trademark Office](#)

[Official Web site for the U.S. Copyright Office](#)

Information on the Fair Use Doctrine:

U.S. Copyright Office, Circular 21, Reproduction of Copyrighted Works by Educators and Librarians,

[www.copyright.gov/circs/circ21.pdf](http://www.copyright.gov/circs/circ21.pdf)

[www.copyright.gov/help/faq/faq-fairuse.html](http://www.copyright.gov/help/faq/faq-fairuse.html)  
<http://www.copyright.gov/fls/fl102.pdf>

[Official Web site for the U.S. Department of Health and Human Services, Office of Civil Rights, on HIPAA](#)

[Official Web site for the U.S. Department of Education,](#)

[Payment Card Industry Data Security Standard \(PCI DSS\)](#)

[Gramm-Leach-Bliley Act](#)

**Information on FERPA:**

[www.ed.gov/policy/gen/guid/fpco/ferpa/](http://www.ed.gov/policy/gen/guid/fpco/ferpa/)

[Student Privacy and FERPA](#)

**FIU IT Security Governance Resources:**

[FIU IT Policies](#)

[Data Classification Policy](#)

[Configuration Management Standard](#)

[Cybersecurity Awareness Standard](#)

[Media Sanitation](#)

[Vendor Risk Management](#)

[Technology Evaluation Group](#)

[FIU Code of Computing Practice](#)

[FIUnet Acceptable Use Policy](#)

[FIU Academic Affairs Policies & Procedures Manual](#)



### CONTACTS

Division of Information Technology  
Information Technology Security Office - PC534  
11200 SW 8 ST, Miami, FL 33199

305-348-1366

### HISTORY

**Initial Effective Date:** May 8, 2006

**Review Dates** (*review performed, no updates*): N/A

**Revision Dates** (*updates made to document*): May 17, 2024