SUBJECT:	**Effective Date:**	**Policy Number:**	
Information Security Policies	9-24-24	12.10	
	Supersedes:	**Page**	**Of**
		1	2
	Responsible Authority: Associate Provost and Chief Information Officer		

I. APPLICABILITY/ACCOUNTABILITY:

This policy defines the process for drafting and implementing policies at the University related to the securing of University technology devices, electronic systems, and the transmission or storage of digital information (collectively, "Information Technology").

II. DEFINITIONS

A. IT Security Policy: A policy relating to the security, control, or compliance-driven management of Information Technology.

B. IT Compliance Committee: A committee established by the University's Chief Information Security Officer (CISO) to discuss and implement security controls to maximize compliance with regulations, laws, security governance needs, or other applicable requirements. The IT Compliance Committee shall consist of the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and representatives from the University Compliance Office, the Office of Information Technology (OIT), IT groups in Colleges, IT groups in HIPAA-covered components, Student Affairs, the Division of Research, Enrollment Management, the Registrar's Office, and Financial Affairs.

III. POLICY STATEMENT:

The CISO will lead the development and implementation of IT Security Policies subject to the procedures and limitations described in this policy. IT Security Policies will apply to all University technology devices and University data subject to the scope defined in each individual policy. IT Security Policies shall not conflict with already established University regulations or policies or other applicable legal or regulatory authorities but may impose additional requirements. In the event of a conflict, University regulations, policies, or other applicable legal or regulatory authorities will take precedence. Policies will be submitted to the IT Compliance Committee for review, and policies will be approved by the CIO.

Policies may be developed that involve shared authority. If such policies are developed, the policy will be submitted to the University Policies and Procedures Committee for review and approval through its existing process, and all applicable authorities will be identified in the policy.

IT Security Policies will apply to HIPAA data and HIPAA-scoped technology devices provided such policies do not weaken any requirement required by established HIPAA policies.

The IT Compliance Committee will be responsible for communicating information on new IT Security Policies to the University. IT Security Policies will be available on the Information Security website: https://www.fau.edu/oit/security.

The CISO will develop and maintain additional internal operational policies governing security that apply to OIT operations and the security of those operations. These policies will generally encompass operational practices, specific controls that need to be updated on a regular basis to reflect changes in risk tolerance, and the implementation of controls needed by other policies. These policies will be regularly reviewed and approved by the CIO.

IV. REFERENCES:

Florida Board of Governors Regulation 3.0075 – Security of Data and Related Information Technology Resources

INITIATING AUTHORITY:

Associate Provost and Chief Information Officer, Office of Information Technology

---

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

Policy Number: 12.10

Initiating Authority
Signature: _____ Date: _____
Name: _____

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: _____

President
Signature: _____ Date: _____
Name: _____

Executed signature pages are available in the Office of Compliance