FLORIDA ATLANTIC UNIVERSITY

Office of the President
University Policy

SUBJECT:	**Effective Date:**	**Policy Number:**	
INFORMATION SECURITY POLICIES	4-15-19	12.10	
	Supersedes:	**Page**	**Of**
	New	1	2
	Responsible Authority: Associate Provost and Chief Information Officer		

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").

DEFINITIONS

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

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 CISO and the CIO, and, at a minimum, representatives from the University Compliance office, OIT, IT groups in Colleges, IT groups in HIPAA-covered entities, Student Affairs, the Division of Research, Enrollment Management, the Registrar's Office, and Financial Affairs.

POLICY STATEMENT:

The CISO will lead the IT Compliance Committee on 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.

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. If

necessary, the University HIPAA Taskforce may define an independent timeline to apply new security controls defined in an IT Security Policy to HIPAA-scoped devices and data provided the independent implementation timeline does not exceed 6 months beyond the implementation of the IT Security Policy.

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

INITIATING AUTHORITY: Associate Provost and Chief Information Officer

---

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

Policy Number: 12.10

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

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

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

Executed signature pages are available in the Office of Compliance