SUBJECT:	**Effective Date:**	**Policy Number:**
INFORMATION SECURITY ROLES AND RESPONSIBILITIES	9-24-24	12.11
	Supersedes:	**Page** **Of**
		1 **4**
	Responsible Authority: Associate Provost and Chief Information Officer	

I. APPLICABILITY/ACCOUNTABILITY:

This policy applies to all faculty, staff, third-party agents of the University, and any other affiliate of the University authorized to access institutional data.

II. DEFINITIONS:

A. Information Security or Security – Protecting and ensuring the confidentiality, integrity, and availability of information or data and any system or device that processes, stores, or accesses information or data.

B. Information Security Program – An overall program designed to support Information Security by defining policies, procedures, guidelines, standards, processes, and operations related to the implementation or support of Information Security.

III. POLICY STATEMENT:

This policy outlines roles to protect sensitive University assets and data from potential compromise, loss, fraud, and abuse. Information Security risk is an institution-wide risk and is ultimately managed by executive leadership. Responsibility for Information Security is shared among all users of FAU technology resources to varying degrees. This policy formally defines Information Security roles and the person(s) primarily designated to carry them out.

A. Chief Information Officer (CIO)

The CIO is responsible for

- Setting the overall strategy for Information Technology at the University
- Supporting the Information Security Program at the University
- Ensuring that an organization-wide Information Security Program is developed and maintained and providing oversight of the program

- Ensuring that Security initiatives are aligned with the strategic vision and goals of the University
- Ensuring that Office of Information Technology (OIT) staff are conducting their responsibilities with the care commensurate with the risk and criticality of the information or systems they are working with
- Reporting to the Provost on an ongoing basis regarding the effectiveness of the Information Security Program at the University
- Reporting to the Board of Governors, Board of Trustees, or other governing body on the effectiveness of the Information Security Program as directed by the University administration
- Ensuring that adequate resources are provided to support ongoing Security and Technology training for Information Security staff based on the availability of University funds and other resources
- Approving or denying proposed Information Security policies

B. Chief Information Security Officer (CISO)

The CISO is responsible for

- Providing Security recommendations to the CIO
- Maintaining an Information Security Plan for the University and updating on an annual basis
- Serving as the Information Security Manager for the University
- Submitting a written report to management on an annual basis covering issues involving risk assessment, risk management, significant security events and violations, management responses to significant security events, and recommendations for changes to the Information Security Program
- Setting the strategy for Information Security based upon directives, goals, and the strategic vision as set by the CIO
- Creating and maintaining Information Security policies, procedures, guidelines, and standards to protect all technology devices and data at the University
- Carrying out Security directives from the CIO
- Monitoring and analyzing Security alerts and information and distributing to appropriate personnel
- Establishing, documenting, and distributing Security incident response procedures as appropriate
- Ensuring that existing Security policy is regularly reviewed and amended
- Organizing an Information Security Awareness Program at the University
- Ensuring that Information Security staff are properly trained and qualified to undertake their responsibilities
- Communicating with University departments regarding Information Security needs and new policies, procedures, guidelines, and standards as appropriate
- Assisting University departments with the implementation of Information Security controls
- Ensuring enforcement and compliance with Information Security policies
- Reporting Compliance failures or concerns to the CIO
- Regularly reporting the effectiveness of the Information Security Program to the CIO

- Establishing and heading an IT Compliance Committee comprised of IT representatives from OIT and other University units
- Performing or contracting periodic risk assessments that identify risks to the confidentiality, integrity, and availability of University information
- Implementing feasible remediation plans to address risks or findings identified in risk assessments or audits
- Implementing a vulnerability management program
- Reviewing and approving all external requests for Level 1, 2, or 3 Information
- Providing advice for mitigating Security risks
- Investigating reports of Security incidents or breaches and reporting any critical incident to the CIO without undue delay
- Maintaining the Information Security of payment card operations
- Monitoring appropriate notification channels to identify current threats and vulnerabilities that may be faced by the institution

C. Departmental/Unit/College IT Managers

IT managers are responsible for

- Ensuring that University-owned devices in their department/unit/college are kept up to date with vendor-supplied Security patches
- Removing University-owned devices in their department/unit/college from the University network when the operating system or firmware is no longer supported by the vendor
- Maintaining an inventory of University-owned technology devices in their department/unit/college
- Implementing Security controls required by the Information Security group on technology devices in their department/unit/college
- Ensuring that members of their department/unit/college are kept informed of changes to Information Security policies.

D. Users

Users are responsible for

- Keeping their personally managed devices up to date with vendor-supplied Security patches
- Reporting lost or stolen university technology devices
- Utilizing a personal firewall on their computers
- Keeping passwords or other account secrets assigned to them secure and not divulging them to any other person
- Completing any Security- or Compliance-related training required by the University
- Complying with all applicable laws and regulations, University policies, and University data management plans relevant to University Information Technology and/or data
- Reporting suspected security incidents to their supervisor or Information Security staff

IV. REFERENCES

University Policy 12.2 – Acceptable Use of Technology Resources

University Policy 12.7 – Systems and Data Classifications

University Policy 12.8 – Payment Card Security

INITIATING AUTHORITY: Associate Provost and Chief Information Officer

---

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

Policy Number: _12.11_

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