Purpose:

To improve the security of University Data and Information Systems by implementing consistent and repeatable information security practices and identifying the roles responsible for developing, approving, and implementing these practices.

Scope:

The policy applies to all University of Florida units that independently manage some aspects of information technology.

Definitions:

University of Florida: The University of Florida, its component units, direct support organizations, and any of its affiliated entities as listed in the University’s annual financial statement.

Unit: A part of the University of Florida that has administrative and financial duties to comply with the university’s information security policies.

UF Senior Leadership: This position is the senior leader of a college or university administrative unit such as a dean, vice president, or director of a unit.

Policy:

1. The university shall develop, annually review, and update an information security plan. The plan may be customized to meet the specific conditions of the university but shall be based upon best practices acquired from recognized national industry standards published by authoritative groups such as: National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA), International Organization of Standards (ISO), Center for Internet Security (CIS), or other nationally recognized information security organizations.

2. Each unit must develop, annually review, and update an information security plan that addresses, at a minimum, the topics identified in the Information Security Plans.
Policy: Information Security Plans

Standard and meets minimum requirements as documented by UFIT. The plan will take into account the scope of the unit’s IT management, and interaction with enterprise-provided IT resources.

Responsibilities:

1. The Chief Information Security Officer is responsible for the development, annual review, update, and implementation of the university’s information security plan.
2. Each Unit’s Director/Manager of IT is responsible for the development, annual review, update, and implementation of the unit’s information security plan.
3. The UF Senior Leadership for each unit is responsible for review and approval of the unit’s information security plan and updates.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

BOG Regulation 3.0075
NIST 800-53: PM-1, PM-2
NIST Cybersecurity Framework (CSF)
UF Information Security Plans Standard