Policy: Information Security Risk Management

Purpose:

To establish a process to manage risks to the University of Florida that result from threats to the confidentiality, integrity and availability of University Data and **Information Systems**.

Scope:

This policy applies to all electronic data created, stored, processed or transmitted by the University of Florida, and the **Information Systems** used with that data.

Policy:

1. All **Information Systems** must be assessed for risk to the University of Florida that results from threats to the integrity, availability and confidentiality of **University of Florida Data**. Assessments must be completed prior to purchase of, or significant changes to, an Information System; and at least every 2 years for systems that store, process or transmit Restricted Data.

2. Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.

3. Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by the Chief Privacy Officer and Chief Information Security Officer. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.

4. Each **Information System** must have a system security plan, prepared using input from risk, security and vulnerability assessments.

Responsibilities:

1. Information Security Administrators (ISAs) are responsible for ensuring that their unit conducts risk assessments on Information Systems, and uses the university approved process.

2. Information Security Managers (ISMs) are responsible for assessing and mitigating risks using the university approved process.
3. Information System Owners (ISOs) are responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred or accepted.
4. The Vice President and Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

NIST 800-53 revision 3: RA-3, CA-2, CA-3, PL-5, PM-9, PM-11, PM-10

HIPAA 164.316 (b)(2)(i), 164.316 (b)(2)(ii)

SEC-RM-001.01: Information Security Risk Assessment Standard

SEC-RM-001.02: System Security Plans Standard

SEC-RM-001.03: External IT Vendor Sourcing Standard