UF UNIVERSITY of FLORIDA
Information Technology

Standard: Information Security Risk Assessment

Purpose:

To establish a process for assessing Information Systems for risks to systems and data; documenting and communicating those risks to university leadership to make decisions regarding the treatment or acceptance of those risks. The security and privacy of Restricted Data will be a primary focus of risk assessments.

Standard:

1. Risk assessments will be conducted:
    a. Prior to acquisition of Information Systems.
    b. When an existing Information System undergoes a significant change in technology or use that would affect its risk posture. Examples include significant software upgrades, changes in hosting platforms or vendors, or changes in the data classification or volume of records stored, processed or transmitted by the system.
    c. At least every two years for systems that store, process or transmit Restricted Data and three years for all other systems.
2. The approved university risk assessment process will include the following:
    a. The scope of the assessment.
    b. An assessment of security control implementation.
    c. Report documenting threats, vulnerabilities and risks associated with the Information System.
    d. Recommendations to increase the security posture of the Information System.
3. The Information Security Office will retain Risk Assessment records according to the university records retention schedules and applicable laws.

References:

SEC-RM-001: Information Security Risk Management Policy