UF UNIVERSITY of FLORIDA
Information Technology

Standard: System Security Plans

Purpose:

To describe required elements of a system security plan

Standard:

1. System security plans include the following:
   a. Description of the operational context.
   b. System categorization and information classifications of data to be used with the system, along with supporting justifications for those decisions.
   c. Inventory of the components that constitute the information system.
   d. Connections between the information system and any other systems.
   e. Overview of security requirements.
   f. Security controls that are in place or planned for implementation, including user responsibilities and how users will be trained.
   g. Dates and milestones for implementation of planned security controls, and remediation of vulnerabilities.
2. Security plans must be reviewed and approved by the unit's Information Security Administrator (ISA) and Information Security Manager (ISM).
3. Security plans must be updated as part of any significant upgrades, configuration changes or software development. Plans must also be updated to reflect needed remediation when vulnerabilities or control deficiencies are identified. Security plans must be reviewed and updated at least every three years.

References:

SEC-RM-001: Information Security Risk Management Policy