Information Security General Provisions:

The purpose as stated by the University of Florida is to delineate the general provisions of information security.

General Provisions

1. **GP0003.04**, General Provisions (Information Security Program Definitions)

Recommendations:

1) Update of the referenced glossary of terms. In addition, IT security administrator should perform glossary updates as needed.

    a) Knowledge, Skills, and Abilities (KSAs) are the skills required to perform a job and are generally demonstrated through relevant experience, education, or training. The Information Security Management Team insures KSAs are defined, comprehension on behalf of management and non-IT is functional and training is ongoing.
    b) A handbook either digital, in print or preferably both, needs to be developed that is more comprehensive than the current article GP0003.04. There are several different information security threats not currently listed. This needs to be addressed immediately. The handbook will be based on the KSA principles found in NICE Cybersecurity Workforce.

2. **GP0007.01/GP0007.02**, General Provisions (SPICE POLICY and Standard Authority)

Recommendations:

1) Update policy as it applies to information classification, security program definitions, violation levels, and report distribution.

a) Categories and descriptions of duties/responsibilities need to be developed and assigned to appropriate IT support staff as well as non-IT staff.
b) Upon development of an IT infrastructure, proper authorization regarding student records needs to be determined and administered to maintain Federal and State compliance.

3. **GP0003.02/GP0003.04/GP0003.06/GP0003.08, (**Information Classification, Information Security Program, Information Security Violations Levels, Report Distribution, and Deadlines)

Recommendations:

1. Update of policy regarding information classification, security, and penalties for non-compliance to information security policy. In addition, establish deadlines for information security reporting as it relates to violations and threats.
    a) A revision of information security responsibility policy to further define chain of custody as it relates to student and university information. As it exists, it is too vague and does not provide sufficient protection to intellectual property of the university or general information of students and faculty.
    b) Established definitions of what constitutes a violation of University information security policy. i.e., Is downloading illegally distributed media on my personal device through a university network grounds for immediate expulsion?
    c) The creation of a report, as well as regularly scheduled physical meetings with university decision makers regarding the status of information security practices and incidents. The report must be an audit itself, and have defined goals or benchmarks. It should be thorough in its scope, and include the physical assets of the university that are related to information security.