UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: GP0003.02	Category: General Provisions	Version Date: 7/15/2004
Title: Information Classification		Effective Date: 3/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review:
Review Resp: HSC Chief, Information Security		Next Review:

Purpose:

The purpose of this Information Classification Standard is to provide a framework for protecting UF Health Science Center (UF HSC) information. Consistent use of this classification system will facilitate business activities and help keep the costs for information security to a minimum.

Reference:

1. Florida Statute, Chapter 119 - Public Records

Standard:

This standard is not intended to nor does it impinge upon the provisions of the Florida Statute, Chapter 119 - Public Records.

In order to protect information from unauthorized disclosure, use, modification, and deletion, an information classification system has been designed as follows (see below for definitions):

- Restricted – Highest level.
- Sensitive – Second highest level.
- Operational – Third highest level.
- Unrestricted – Lowest level.

No distinctions are made for purposes of this standard between the words: data, information, knowledge, and wisdom. Information must be consistently protected throughout its life cycle, from its origination to its destruction. It also must be protected in a manner commensurate with its sensitivity regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this standard provides overall guidance, to achieve consistent information protection users will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

Aggregates of information should be classified as to the most secure classification level of an individual information component within the aggregated information (e.g., when information of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of any individual data element within the content of the database, file, or report).

Definitions:

- **Restricted** - information whose loss, corruption or unauthorized disclosure, would seriously and adversely impact the academic, business or research functions of UF HSC. The impacts on UF HSC could include any violation of privacy, business, financial, legal or other contracts, or a violation of federal or state laws/regulations. Examples include, but are not limited to, statutorily protected medical information, patient medical charts, and litigation documents.
- **Sensitive** - information whose loss, corruption or unauthorized disclosure would tend to impair the business or research functions of UF HSC, or result in potential business, financial, or legal loss. Examples include medical information (except that which is restricted), appointment schedules, department financial information, purchasing information, and UF HSC strategy documents.
- **Operational** - information whose loss, corruption or unauthorized disclosure would result in minimal business, financial or legal loss BUT involves issues of convenience, ease of operation, personal credibility, reputation, or other issues of personal privacy. Examples include phone directories, internal training materials, and internal policy manuals.
- **Unrestricted** - information that does not fall into any of the other information classifications. This information may be made generally available without specific information owner's designee or delegate approval. Examples include advertisements, job opening announcements, and press releases.

Security Requirements:

	Restricted	Sensitive	Operational	Unrestricted
Information Integrity	Vital.	Vital.	Important but not vital.	Not vital.
Loss of Service	Not acceptable.	Not acceptable.	Acceptable for some period of time.	Acceptable.
Access Protocol	Limited to as few persons as possible, on a need to know basis; Access controls are mandatory, adhering to applicable policies or required by state and/or federal law,	Limited to as few persons as possible, on a need to know basis; Access controls are mandatory, adhering to applicable policies or required by state and/or federal law,	Available on a need to know basis; Access controls are discretionary as determined by the owner's designee or delegate for the	Available to the general public; no access controls.

	and are not determined by the owner's designee or delegate for the application.	and are not determined by the owner's designee or delegate for the application.	application.	
Encryption	Required if transmitted through any un-trusted network, including the Internet.	Required if transmitted through any un-trusted network, including the Internet.	Encouraged if transmitted through any un-trusted network, including the Internet.	Not required.
Auditing	All access is to be monitored and logged for off-line scrutiny (real-time when feasible) and in compliance with regulatory requirements. Intrusion Detection mechanisms must be implemented. All unsuccessful access requests are reported to security personnel for action in a manner commensurate with the criticality of the information.	All access is to be logged for later scrutiny. Intrusion Detection mechanisms should be implemented.	All access is to be logged and monitored as determined by the information owner's designee or delegate.	None.