Guidelines: Data Classification

The Data Classification Policy specifies that all university data must be assigned one of three levels based upon confidentiality requirements: Open, Sensitive or Restricted. Data owners are given the responsibility of appropriately classifying data.

The classification should be a list of specific data types used within a unit, corresponding classifications, and any special handling specifications. The task of preparing the classification may be delegated, but the data owner must explicitly approve the final document. This classification must be documented and communicated with data users and custodians. Data custodians then apply appropriate controls based on these classifications, and data users comply with the use requirements.

Controls appropriate to the different data classifications are specified in information security policies and standards. Data classifications, including 'Open', are not related to the applicability of public records laws to specific data. All requests for public records are to be forwarded to the University General Council, regardless of the classification of requested data.

Initial Classification:

Data owners can use the table below as an initial classification of data within their unit. Data types that have classifications mandated (due to applicable laws, regulations or contracts) and those that are in common use throughout the university are included. Data owners must add any other data types used in the unit.

Data Type	Classification	Justification
Student records (non-directory)	Restricted	FERPA
Credit card cardholder data	Restricted	PCI, FS 817.5681
Patient medical records (identifiable)	Restricted	HIPAA
Patient billing records	Restricted	HIPAA
Social Security Numbers[1]	Restricted	FS 817.5681
Export Controlled data	Restricted	ITAR
Animal research protocols	Sensitive	Competitive and commercial potential, security concerns
System security plans	Sensitive	Protective information
Unpublished research results	Sensitive	Competitive and commercial potential

[1] Use and/or storage of social security numbers must be approved by the UF Privacy Office. See http://privacy.ufl.edu/SSNPrivacy.html

Exams (questions and answers)	Sensitive	Exam integrity
Employee data (not including SSN)	Sensitive	Employee privacy
UF Directory (students & staff)	Open	FERPA
University regulations	Open	Intended for public use
Course catalog	Open	Intended for public use
Public web sites	Open	Intended for public use
De-identified patient information[2]	Open	HIPAA

Definitions:

Data owner: Senior leadership, typically at the dean, director or department chair level, with the ultimate responsibility for the use and protection of university data.

Data custodian: The staff member, typically one primarily responsible for IT, that is responsible for implementation of security controls for university data.

Data user: Any member of the university community that has access to university data, and thus is entrusted with the protection of that data.

References:

UF Data Classification Policy:
http://www.it.ufl.edu/policies/dataclassificationpolicy.html

HIPAA: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

FERPA: http://privacy.ufl.edu/studentfaculty.html

PCI: https://www.pcisecuritystandards.org/

[2] In order to be considered de-identified, data must meet requirements in the UF Privacy Office Operational Guidelines http://privacy.health.ufl.edu/policies/hipaamanual/opguide/UF-Operations07-01-10-Web.pdf

Florida Statute 817.5681 Breach of security concerning confidential personal information in third-party possession:
http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.5681.html

ITAR: http://www.pmddtc.state.gov/regulations_laws/itar.html