Authority
This standard was enacted by the UF Senior Vice President for Administration and the UF Interim Chief Information Officer on July 10, 2008 [16]. It was approved by the UF Chief Privacy Officer and UF General Counsel.

Who Should Know This
- Deans, Directors, Department Chairs
- IT Workers authorized to implement security controls to protect Restricted Data
- Users authorized to access Restricted Data

Summary
These standards define terms important for understanding protection of Restricted Data. Only the electronic and technological aspects of protecting Restricted Data confidentiality are addressed. Roles are defined and their relationship to data protection is explained.

Definitions
- Restricted Data: Data, which if disclosed to unauthorized users, may have very significant adverse operational or strategic impact on an individual, a group or institution. This classification includes, but is not limited to, data restricted by law and legal contracts. Data commonly called private data usually falls in this classification. Examples include, but are not limited to, social security numbers, credit card numbers, bank account numbers, drivers license number, student grades, and medical records.
- Restricted Data Type: Restricted Data is categorized into groups sharing common characteristics, protection requirements and use limitations [12,13,14]. For instance, Student Educational Records [11] is a Restricted Data Type that includes biographical data, grades, coursework, disciplinary information, financial information, and information about internships. Protection requirements regarding authorization, recoverability, and limitations for use on portable devices and removable media may vary for each Restricted Data Type.
- Data Principal: Unit administrators (Deans, Directors, and Department Chairs, also called DDD) with authority to direct action as needed to protect UF Restricted Data and enforce UF and unit data security policies, standards, and procedures.
- Data Custodian: Professional IT workers who provide technical facilities and support services to Data Principals and Data Users. Data Custodians implement security controls to protect data.
- Data User: Anyone authorized to access, create or alter Restricted Data.

Purpose and Scope
These standards are intended to convey the specifications for protection of Restricted Data. Other data may also need protection and is addressed by other UF regulations.
These standards address only data confidentiality. Other UF regulations address data integrity or availability.

These standards address only the electronic and technological aspects of data security. Security of paper documents, physical security of servers and network infrastructure, and many other aspects of general data security are addressed by other UF regulations.

Identification of Restricted Data Types and their use limitations are covered in other standards [12, 13, 14].

**Data Principal Standards**
1. Deans, Directors, Department Chairs are Data Principals. They enforce UF and unit policies and procedures for creating, altering, transmitting and storing Restricted Data used under their direction.
2. Data Principals must formally authorize and document Data Custodians in their unit who implement security controls. They coordinate with Data Custodians to ensure effective security controls are implemented.
3. Data Principals must formally authorize and document Data Users in their unit who access, create, alter or delete Restricted Data. They must ensure Data Users comply with their responsibilities to protect Restricted Data.
4. Data Principals must formally authorize and document IT devices that are used with Restricted Data.
5. Data Principals must ensure that appropriate awareness material is available to Data Custodians and Data Users explaining their obligations to protect the data. Data Principals must ensure Data Custodians and Data Users attend data security training provided and required by UF. Compliance and/or training certification may also be required.
6. If loss or unauthorized exposure of Restricted Data is discovered, the incident must be immediately reported to the UF Privacy Office [3]. For detailed incident response procedures, see the UF IT Security Incident Response Procedures, Standards and Guidelines [15].

**Data Custodian Standards**
1. IT workers who implement controls to protect Restricted Data must be authorized by the Data Principal (Dean, Director, or Department Chair) in their unit.
2. Data Custodians should assist the Data Principal in their unit with cost-effectiveness evaluation of security controls.
3. Data Custodians are accountable for their actions regarding Restricted Data handling. They may be subject to penalties and disciplinary action, both within and outside the university. Violations will be handled through the university disciplinary procedures applicable to the relevant Unit or IT worker.
4. Data Custodians must maintain an accountability of who is authorized to access Restricted Data and at least annually revalidate the access requirements.
5. Data Custodians must document, implement, and verify that server, operating system, network, workstation, and application controls are commensurate with the following requirements to protect Restricted Data confidentiality.
   a. Restricted Data must reside on an appropriately secured host [4].
   b. Locations where Restricted Data resides must be appropriately secured [5].
c. Restricted Data must be available only to those who are authorized and authenticated. Access controls should be based on the minimum necessary and least privilege principles.
d. Facilities must be available for users to securely store and transmit Restricted Data preventing unauthorized access [7].
e. Restricted Data must be rendered unreadable prior to disposal [6, 8]. Disposal must be consistent with Florida record retention requirements [2].
f. Encryption needs for the data must be addressed according to contractual and regulatory requirements such as HIPAA [10], Florida Statute 817.5681 [1], and the Payment Card Industry standards [9].
g. Use of access logs must be addressed according to contractual and regulatory requirements such as HIPAA [10] and the Payment Card Industry standards [9].

6. If loss or unauthorized exposure of Restricted Data is discovered, the incident must be immediately reported to the Data Principal and the UF Privacy Office [3]. For detailed incident response procedures, see the UF IT Security Incident Response Procedures, Standards and Guidelines [15].

Data User Standards
1. Data Users must be authorized to access Restricted Data by the Data Principal (Dean, Director, or Department Chair) in their unit.
2. Data Users must comply with applicable UF and unit policies, standards and procedures to manage UF Restricted Data. UF training is available to help users understand their responsibilities. Compliance and/or training certification may be required.
3. Restricted Data Users are accountable for their actions regarding Restricted Data handling [12, 13]. They may be subject to penalties and disciplinary action, both within and outside the university. Violations will be handled through the university disciplinary procedures applicable to the relevant Unit or employee.
4. Restricted Data must be created, altered or deleted using only computers and applications approved by the Level 2 Unit ISM.
5. If loss or unauthorized exposure of Restricted Data is discovered, Data Users must immediately report the incident to the Data Principal and the UF Privacy Office [3], usually through their supervisor.

Bibliography
[12] Standards for Private Educational Record Data Use Limitations: <link>
[13] Standards for Personally Identifiable Information Use Limitations: <link>