

<b>SUBJECT:</b> Data Classification and Protection	<b>Effective Date:</b> 11-5-07	<b>Policy Number:</b> 4-008
	<b>Supersedes:</b>	<b>Page</b> <b>Of</b> <b>1</b> <b>4</b>
	<b>Responsible Authority:</b> Vice Provost for Information Technologies & Resources	

**APPLICABILITY/ACCOUNTABILITY:**

This policy applies to all employees of the University of Central Florida who maintain or use university data.

**POLICY STATEMENT:**

Data are critical assets of the university. All members of the university community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the university, irrespective of the medium on which the data resides, such as electronic, paper, or other physical form. It is the policy of the University of Central Florida to classify types of data in use at the university and to provide the appropriate levels of information security and protection.

**DEFINITIONS:**

Data. Numerical or other information represented either in a physical form or a form suitable for electronic processing or storage.

Family Educational Rights and Privacy Act of 1974, also known as the Buckley Amendment. FERPA is a federal law that protects the privacy of student academic records.

Gramm-Leach Bliley Act. GLBA is a federal law that protects consumers' personal financial information held by financial institutions, including universities.

Health Insurance Portability and Accountability Act of 1996. HIPAA protects the security of individually identifiable health information.

Institutional data. All data created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf.

Network identification. A UCF-issued credential to be used by university employees and students to access systems that do not contain restricted data. NIDs are classified as unrestricted data.

Personal identification. A UCF-issued credential to be used by university employees and students to access systems that contain restricted data. PIDs are classified as restricted data.

Restricted data. Data that are considered sensitive and protected. There are two subclassifications of restricted data: personal and non-personal.

Personal restricted data includes personally identifiable information: a) information from which an individual may be uniquely and reliably identified or contacted, including an individual's social security number, account relationships, account numbers, account balances, account histories, and passwords; b) information concerning an individual that is considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 11 Stat. 1338) (as amended) and its implementing regulations, and; c) information concerning an individual that is considered "protected health information" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended), and its implementing regulations. Protection for such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.

Personal restricted data also include the home addresses, telephone numbers, social security numbers, and photographs of certain university employees, such as police officers and their spouses, as specified in F.S. 119.07(4)(d)1-7.

Non-personal restricted data includes electronic information whose unauthorized access, modification, or loss could adversely affect the university; e.g., cause financial loss or loss of confidence or public standing in the community, adversely affect a partner; e.g., a business or agency working with the university, or adversely affect the public.

Non-personal restricted data also includes security-related information, such as computer passwords and student academic records as defined by the Family Educational Rights and Privacy Act of 1974.

Secure sockets layer. A protocol for securing data received from or sent to Web sites. SSL-secured Web pages will display a padlock symbol in the Web browser.

Strong password. A password that is difficult to guess, consisting of six or more characters including numbers and specials characters.

Unrestricted data. Data that are not regarded as restricted, are not protected by law or contract, or whose disclosure would cause no harm to the university or to individuals.

Virtual private network. A secure means of connecting to a private network, such as the UCF network, from or through an insecure public network, such as the Internet or a wireless network. VPNs encrypt data during transmission.

#### PROCEDURES:

University employees who create, view, and manage university data are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of university data in compliance with this policy. Data owned, used, created, or maintained by the university are classified into the following categories:

- Restricted Data
  - Personal Restricted Data
  - Non-personal Restricted Data
- Unrestricted Data

#### Restricted data:

- when stored in an electronic format, must be protected with strong passwords and stored on secured servers to protect against loss, theft, unauthorized access, and unauthorized disclosure.
- when in “hard copy” format or recorded on mobile electronic media, must be stored in a locked cabinet or drawer in a room or an area where access is controlled by a lock or card reader or that otherwise has sufficient physical access control measures to prevent unauthorized access by members of the public, visitors, or other persons without a need to know.
- when transmitted through a data network, must always be protected by using a secure connection method, such as a VPN or SSL.
- must not be disclosed to parties without explicit management authorization and then only on a need-to-know basis.
- when sent via fax, must be sent only to a previously established and used address or one that has been verified as being in a secured location.
- must be accessed using the PID, or similarly secure credential, with a strong password; passwords on systems holding confidential data must be changed every 60 days or less.
- must not be posted on any public Web site.
- must be destroyed when no longer needed, subject to the records retention schedule. Destruction may be accomplished in the following manner:
  - "Hard copy" materials must be destroyed by shredding or another process that destroys the data beyond recognition or reconstruction. After destruction, materials may be disposed of with normal waste.

- Electronic storage media shall be sanitized appropriately by degaussing prior to disposal or by physical destruction of storage media.

The UCF Information Security Officer must be notified immediately if data classified as restricted is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the university's information systems is occurring or is suspected of having occurred.

All public records requests for university data should be processed according to UCF Policy 2-100.1 *Florida Public Records Act – Scope and Compliance*.

Court orders, subpoenas, or requests of federal or state agencies for access to university data should be referred to the Office of the General Counsel.

Copyrighted data must be handled according to applicable federal copyright laws and UCF policy 2-103 *Use of Copyrighted Material*.

RELATED DOCUMENTS:

2.100.1 *Florida Public Records Act—Scope and Compliance* policy

2-103 *Use of Copyrighted Material* policy

3-206.1 *Cardholder Information Security Procedures* policy

4-007 *Security of Mobile Computing, Data Storage, and Communication Devices* policy

Records retention schedule - <http://dls.dos.state.fl.us/barm/genschedules/g505.doc>

CONTACTS:

Computer Services and Telecommunications, Information Security Officer, 407-823-3863

INITIATING AUTHORITY: Provost and Executive Vice President

POLICY APPROVAL	
(For use by the Office of the President)	
Policy Number: <b>4-008</b>	
Initiating Authority: <i>[Signature]</i>	Date: <i>12/4/07</i>
Policies and Procedures Review Committee Chair: <i>[Signature]</i>	Date: <i>12.3.07</i>
President or Designee: <i>[Signature]</i>	Date: <i>12/4/07</i>