

NOTICE OF PROPOSED REGULATION

Date: October 25, 2012

REGULATION TITLE:
Sensitive Information Disclosure

REGULATION NO.:
UCF-3.045

SUMMARY OF PROPOSED REGULATION: This new regulation defines the role of employees concerning sensitive information and its unauthorized use or disclosure.

AUTHORITY: BOG Regulation 1.001

NAME OF PERSON WHO INITIATED PROPOSED REGULATION:
Mark Roberts, Assistant Vice President, Chief Human Resources Officer

COMMENTS CONCERNING THE PROPOSED REGULATION SHOULD BE SUBMITTED WITHIN 14 DAYS OF THE DATE OF THIS NOTICE TO THE CONTACT PERSON IDENTIFIED BELOW. The comments must identify the regulation you are commenting on.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED REGULATION IS:

Regulations Administrator
4000 Central Florida Blvd.
Millican Hall, Suite 360
Orlando, FL 32816-0015
Phone: (407) 823-2482
Fax: (407) 823-6155
e-mail: regulations@mail.ucf.edu

FULL TEXT OF THE PROPOSED REGULATION:

UCF-3.045 Sensitive Information Disclosure

(1) The University receives, creates, or has custody of various categories of information. Further, the University is responsible for securing sensitive information from unauthorized use and/or disclosure.

(2) This regulation applies to all full and part-time faculty and staff university employees, student workers, and affiliates and governs all information acquired during the course of employment or service to the university including that which may be subject to Florida Statutes, Chapter 119.

(a) University employees, student workers, and affiliates have a duty to protect all sensitive information acquired during the course of employment or service to the University of Central Florida.

1. A university employee is a person employed to perform duties or services for the university.
2. A student worker is a student that is employed to perform duties or services for the university.
3. An affiliate is an individual or entity not directly employed by the University, but who is granted access to confidential information for the purpose of performing services for the university. An “affiliate” may be paid or unpaid. An individual performing volunteer services for the University is an “affiliate.”
4. Sensitive Information includes, but is not limited to, the following categories of information, regardless of the format or medium in which the information is made, kept, or received (i.e., paper, electronic, video, verbal, etc.): any personally-identifiable student or parent information, financial information (including social security and credit card numbers), or health information; certain contracts; research information; alumni and donor information; personnel information other than an individual’s own personnel information; university financial information; computer passwords; university proprietary information; and any other information for which access, use, or disclosure is not authorized by university regulation, policy, or procedure.

(b) Each employee, affiliate, student, or other person in any capacity who has access to information, holds a position of trust and must preserve the security and confidentiality of the information that he or she uses.

- (c) Users of university data and information are required to abide by all applicable Federal and State laws and university regulations, policies, or procedures regarding protection of data and information, including UCF Policy 4-008, Data Classification and Protection.

(2) The following principles shall govern Sensitive Information handling at UCF.

- (a) Documents and files (both electronic and hard copy) containing Sensitive Information are to be accessed, used, and/or disclosed only with explicit authorization and only on a need-to-know basis for purposes of the employee's job function or the affiliate's service.
- (b) University resources must not be used to obtain, store, or transmit Sensitive Information regarding any individual or entity without authorization.
- (c) Sensitive Information acquired during the course of employment or service the university must not be divulged to anyone outside of the university without authorization or to anyone within the university without the need-to-know.
- (d) Based on record retention requirements, documents and files containing Sensitive Information must be disposed of in a way that ensures that the information is no longer recognizable or retrievable.
- (e) All employees, student workers, and affiliates have a duty to use available physical, technological, and administrative safeguards, in accordance with university regulations, policies, and procedures, to protect the security of Sensitive Information regardless of form or medium.
- (f) Upon conclusion of an employee's or student worker's employment or an affiliate's service, or upon request of an appropriate supervisor: the employee, student worker, or affiliate will return originals and copies of information (regardless of medium) containing Sensitive Information to the university and terminate all further access to and use of such information.
- (g) Employees, student workers, or affiliates who disclose Sensitive Information to any unauthorized person, breach confidentiality, or abuse their position relating to Sensitive Information could be subject to disciplinary action, up to and including dismissal, depending upon the circumstances of the violation.

(3) Applicability of Certain Federal Laws

- (a) Family Educational Rights and Privacy Act (FERPA). By circumstance of employment at or service to UCF, an individual is likely to gain access to student education information or to personally identifiable information about students. Such information is governed and restricted both by FERPA and Florida statute.
 - (b) Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA protects the security of individually identifiable health information in most healthcare and health-related settings. The University has various departments that are engaged in health-related services or which may receive health-related information about individuals. Access to and disclosure of such information may be restricted by HIPAA and/or state law.
 - (c) Gramm-Leach Bliley Act (GLBA). The GLBA is a federal law that protects consumers' personal financial information held by the University. The University may obtain personal financial information about an individual during the ordinary course of University business (for example, in calculating financial aid packages). Access to and disclosure of such information is restricted by GLBA.
- (4) An individual unit may require its employees and affiliates to sign a unit-specific confidentiality agreement so long as its conditions do not conflict with those contained in this regulation, or with applicable federal or state law.
- (5) Employees are advised to refer to and abide by UCF Policy 4-008 Data Classification and Protection, which contains additional information relating to data classification and protection.