FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

University Community (faculty, staff and students) and Authorized Users of University's IT Resources (e.g., consultants, vendors, visitors, contractors, etc.)

SUBJECT (R*)	EFFECTIVE DATE (R)	PROCEDURE NUMBER
DATA STEWARDSHIP	October 2007	1930.020a

PROCEDURE STATEMENT (R)

University employees, students and authorized users of the University's IT resources (e.g. consultants, vendors, visitors, and contractors) shall access and use Highly Sensitive Data only as may be strictly necessary in the performance of their job or role at the institution and in accordance with all applicable state and federal laws. All individuals accessing Highly Sensitive Data created or maintained by Florida International University are required to comply with federal and state laws and university policies and procedures regarding data security. Any University employee, student or non-University individual with access to Highly Sensitive Data created or maintained by the University who engages in the unauthorized use, disclosure, alteration, or destruction of same is in violation of state and federal laws.

Access to University data is provided to University employees for the conduct of University business. Highly Sensitive University data, as defined in this procedure, will be made available to employees who have a genuine need to access such data. This may include data collected from students, faculty, staff, donors, contractors, members of the community, or those who have no affiliation with the University. It is the responsibility of each individual to which this procedure applies accessing such data to observe the following:

All Highly Sensitive Data should be handled as follows:

Hard Copy - these documents should never be stored temporarily or permanently where unauthorized individuals can have access to read, copy or photograph. It is necessary to store these documents in file cabinets that have locks and that are located in an area that is locked except during normal business hours.

Electronic Copy –

1. All Highly Sensitive Data must be accessed by way of a unique name or number for identifying and tracking user identity.
2. Highly Sensitive Data stored in electronic format must be encrypted using a minimum of 128 bit encryption. This applies to all local and shared drives.
3. Departments/Divisions that maintain Highly Sensitive Data must coordinate with University Technology Services to ensure that they have procedures in place that will allow them to access Highly Sensitive Data in the event of an emergency.

REASON FOR PROCEDURE (O*)

Florida International University creates and maintains data which, while essential to the performance of University business, consists of information and data elements the privacy and confidentiality of which are protected by state and federal laws. The University must ensure that it has in place the necessary administrative, technical and physical safeguards in order to ensure that the privacy and confidentiality of these data.

RELATED INFORMATION (O*)

Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. § 1232g
FIU 108 – FIU Board of Trustees Access to Student Education Records Regulation
Florida Statutes §1002.21 (Postsecondary student and parent rights), §1002.22 (Student records and reports), §1006.52 (Student Records)

Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191
HIPAA Security Standards, 42 CFR §164.312
University IT Policy: Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information
University IT Policy: Information Technology Security

DEFINITION (R)

Hard Copy: A permanent reproduction, on any media (in particular paper) suitable for direct use by a person, of displayed or transmitted data.

Highly Sensitive Data is defined as information which must be protected from disclosure by state or federal law, or by binding contractual arrangement. Among the types of data included in this category are individually identifiable financial or health information, social security numbers, credit card information, student education records and proprietary data protected by law or agreement.

Electronic Copy: An electronic version of a document or file.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology
Florida International University

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

FIU IT Security Office
Biscayne Bay Campus, LIB 328
3000 N.E. 151st Street
Miami, Florida 33181
Telephone Number: (305) 919-4299

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at http://policies.fiu.edu/.

For any questions or comments, the "Document Details" view for this procedure online provides complete contact information.

R*=Required O*=Optional