University employees, students and authorized users of the University’s IT resources (e.g. consultants, vendors, visitors, 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.
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

DEFINITIONS (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.

HISTORY (R*)

Initial Effective Date: October 2007; December 31, 2017

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

FIU IT Security Officer
Biscayne Bay Campus, LIB 328 3000 N.E. 151st Street
North 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.

FORMS/ONLINE PROCESSES (O)

Links to the above referenced Form(s) available in the "Document Details" Section of the online version of this policy document.

*R = Required  *O = Optional