FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Data Stewardship # 1930.024

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	June 9, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

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/Confidential 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/Confidential 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 employees, student or non-University individual with access to Highly Sensitive/Confidential 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/Confidential data 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.

SCOPE

University Faculty, Staff, Students, Person of Interest, Vendors, and Contractors

REASON FOR POLICY

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.

DEFINITIONS	
TERM	**DEFINITIONS**
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/Confidential 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.
University Data	Information generated by or for, owned by, or otherwise in possession of Florida International University that is related to University's Activities.
Data Steward	All FIU employees, students and authorized users of IT data resources.
Data Owner	Any manager, director, division head or equivalent, who has accountability and responsibility for the integrity, accurate reporting and use of computerized data. This individual(s) typically exists within the department that generated the data and is ultimately accountable for its accuracy and proper handling.
Data Consumer	The individual(s) and department(s) that use provided data to perform a job responsibility including the possible generation of new data. A data consumer may also be a data steward if that person transfers data from its original location. Example: If an employee or contingent worker transfers data from a server or website to their workstation, that individual is not only a consumer but also a steward of that data and is responsible for its proper handling.

ROLES AND RESPONSIBILITIES

It is the responsibility of each individual to which this procedure applies accessing such data to observe the following:

All Highly Sensitive/Confidential Data should be handled as follows:

Hard Copy –

1. These documents should never be stored temporarily or permanently where unauthorized individuals can have access to read, copy or photograph.

2. 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.
3. These documents must be shredded with a crosscut shredder when no longer in use or required.

Electronic Copy –

1. All Highly Sensitive/Confidential Data must be accessed by way of a unique name or number for identifying and tracking user identity.
2. To maintain its confidentiality, Highly Sensitive/Confidential Data stored in electronic format must be encrypted while in transit or when stored on IT resources.
3. To maintain its confidentiality, Highly Sensitive/Confidential Data shall not be stored on local workstations, external drives, or personal devices.
4. Departments/Divisions that maintain Highly Sensitive/Confidential Data must coordinate with Division of Information Technology, IT Security Office to ensure that they have procedures in place that will allow them to access Highly Sensitive/Confidential Data in the event of an emergency.
5. Follow data destruction and retention policies.

System Admins shall implement access controls on all IT resources that store, transmit, or process highly sensitive/confidential data.

University Departments and Units that store, processes, or transmits Highly Sensitive/Confidential Data will create a plan to safeguard IT resources from physical tampering, damage, theft, or unauthorized physical access.

RELATED RESOURCES

U.S. Department of Commerce Export Controls
General Data Protection Regulation (GDPR)
Federal Information Security Modernization Act of 2014 (FISMA)
Executive Order 13556 "Controlled Unclassified Information"
32 CFR Part 2002 "Controlled Unclassified Information"
Protecting Unclassified Information in Nonfederal Information Systems and Organizations (NIST SP 800-171r1)
Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53, Rev 4)
Assessing Security Requirements for Controlled Unclassified Information (NIST SP 800-171A)
U.S. Dept of Health HIPAA website
Health and Human Services Information for Covered Entities
PCI Security Standards Council
Federal Trade Commission: Gramm-Leach-Bliley Act
Federal Standards for Safeguarding Customer Information

U.S. Department of Education

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 ST, PC534A
Miami, FL 33199
305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: October 2007
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): June 9, 2021 (formerly 1930.020a procedure converted into separate policy and procedure)

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Data Stewardship # 1930.024a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	June 9, 2021	Division of Information Technology/IT Security Office

PROCEDURE STATEMENT

Data Consumers, Data Stewards, and Data Owners must complete the Annual Cybersecurity Awareness training each year.

All Highly Sensitive/Confidential Data should be handled as follows:

Hard Copy:

1. These documents should never be stored temporarily or permanently where unauthorized individuals can have access to read, copy or photograph.
2. 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.
3. These documents must be shredded with a crosscut shredder when no longer in use or required.

Electronic Copy:

1. All Highly Sensitive/Confidential Data must be accessed by way of a unique name or number for identifying and tracking user identity.
2. To maintain its confidentiality, Highly Sensitive/Confidential Data stored in electronic format must be encrypted while in transit or when stored on IT resources.
3. To maintain its confidentiality, Highly Sensitive/Confidential Data shall not be stored on local workstations, external drives, or personal devices.
4. Departments/Divisions that maintain Highly Sensitive/Confidential Data must coordinate with Division of Information Technology, IT Security Office to ensure that they have procedures in place that will allow them to access Highly Sensitive/Confidential Data in the event of an emergency.
5. Follow data destruction and retention policies.