FLORIDA
INTERNATIONAL
UNIVERSITY

Data Classification Standard

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
Month/Day/Year The date on which the policy was initially adopted.	Month/Day/Year Date of last revision or review of policy by policy owner. (this will be the date of the current review)	The University Division/Department whose jurisdiction covers the subject matter of the policy. This is the subject matter expert and is responsible for policy administration, interpretation, general questions and compliance efforts related to the policy.

Classification Standard

FIU's Data stored in electronical form are vital assets and should be protected as such. FIU has established a Data Classification guideline to assist departments and IT administrators in providing the necessary security controls required for data security. This guideline exists in addition to all other university policies and federal and state regulations governing the protection of the university's data. Three data classifications were established and a set of security standards are delineated to protect the confidentiality, integrity and availability of information.

Data classification establishes a criteria for data identity. These classifications drive the security controls that will be applied to the data. By creating actionable data security and controls around FIU's data, the Division of Information Technology will be able to assist departments take the steps necessary for protecting the university's intellectual assets, as well as data entrusted to FIU for business use. FIU's data classification places data in one of 3 levels. Level 3 being the highest level of sensitivity, thus requiring the highest level of security controls. Level 1 being the lowest level of sensitivity, requiring less stringent controls.

Level 3 – Confidential Data

Data is classified as level III – Confidential Data

Confidential Data is applied to highly sensitive data and is intended for use only by authorized individuals. Data in this classification is regulated by legal standards and inappropriate use or disclosure could result in monetary fines to FIU.

Examples include, but are not limited to information covered under FERPA, GLBA, PCI, HIPAA, CUI and GDPR regulations. Specific data fields such as credit card numbers and social security numbers will fall into this category.

The highest level of security controls must be applied to his classification.

Level 2 – Internal/Private Data

Data is classified as level II – Internal/Private Data

Internal/Private data is assigned to data with a moderate sensitivity, and unauthorized disclosure of the data could result in a negative impact on the university. Data that is not categorized as Confidential or Public will be treated as Internal/Private data and normal security controls should be applied.

Examples of Data that fall into this category include some data sets covered by FERPA regulations, such as student grades; FIU's intellectual property, such as financial data, exam answer files.

Level 1 – Public Data

Data is classified as level I – Public Data

Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the University and its affiliates. While minimal controls are explicitly required to protect the confidentiality of Public data, security controls are equally important to ensure the availability and integrity of the data. The impact on the institution should Level I - Public data not be available is typically low (inconvenient but not a threat to business continuity). This data is publicly available and does not have a requirement for confidentiality, integrity or availability.

Examples of Public data include directory information, course information, and research publications on public facing resources such as an FIU web site.

Data Classification Examples:

Level 3 – Confidential Data

Data is classified as level III – Confidential Data

- Health Information, including protected health information (PHI)
- Social Security numbers
- Credit Card Numbers
- Data of birth
- Personal vehicle information
- User account passwords
- Fingerprints
- Export Control Information
- Passport and visa numbers
- Financial account numbers
- Driver's license numbers
- Donor contact information and non-public gift information
- Health Insurance policy ID numbers
- Controlled Unclassified Information
-

Level 2 – Internal/Private Data

Data is classified as level II – Internal/Private Data

- Student Records
- Admissions Applications

- Panther ID's
- Network designs and operational information regarding FIU's Infrastructure.
- Unpublished research data (at data owner's discretion)
- Employee names
- Employee salary information
- Employee performance information
- Internal memos and email
-

Level 1 – Public Data

Data is classified as level I – Public Data

- Job postings
- University directory Information
- Information in the public domain
- Publicly available campus maps
- Research data (at data owner's discretion)
- Information on FIU's websites without authentication requirements

Based on the **Data Classification Level** the following **Data Security Controls** will vary. The following table of security controls must be implemented unless a control is waived and documented by the IT Security Office.

Data Security Control - Checklist

Control	Confidential Data	Internal/Private Data	Public Data
Policy & Governance	**Required**	**Required (W,S)**	**Not Required**
Personnel Security (background check)	**Required (W,S)**	**Required (W,S)**	**Recommended (W,S)**
Physical Security	**Required (W,S)**	**Required (W,S)**	**Recommended (W,S)**
Inventory Assets	**Required (W,S)**	**Required (W,S)**	**Recommended (W,S)**
Authentication Control (2F) **	**Recommended (W)**	**Recommended (W)**	**Not Required (W)**
Secure Configuration – hardware (Spec. sheet)	**Required (W,S)**	**Recommended (W,S)**	**Recommended (W,S)**
Secure Configuration - software (Spec. sheet)	**Required (W,S)**	**Recommended (W,S)**	**Recommended (W,S)**
Access Control (Unique)	**Required (W,S)**	**Required (W,S)**	**Not Required**
Encryption (At Rest & In T	**Required (W,S)**	**Required (W,S)**	**Recommended (w**
AV/HIPS	**Required (W,S)**	**Required (W,S)**	**Required (FIU devices) (W,S)**
DLP	**Required (W,S)**	**Required (W,S)**	**Not Required**
Firewall (H - host and N - network)	**Required (W,S) H, N**	**Required (W,S) H, N**	**Required (FIU devices) (W,S)(H,N**

Patch Management	**Required (W,S)**	**Required (W,S)**	**Required (FIU devices) (W,S)**
Vulnerability Scanning	**Required (W,S)**	**Required (W,S)**	**Required (W,S)**
Shut Down unnecessary services	**Required (W,S)**	**Required (W,S)**	**Recommended (W,S)**
Mobile Devices *	**Restricted**	**Approval Required (define process)**	**Not Required**
E-mail	**Restricted**	**Allowed (W/Controls)**	**Not Required**
Incident Handling	**Required (NDS)**	**Required**	**Not Required**
Audit and Compliance monitoring	**Required (W,S)**	**Required (W,S)**	**Not Required**

Compliance and Enforcement

Any individual or department found in non-compliance with this policy will be given an immediate mandate to take corrective action. Failure to remediate inappropriate handling of FIU data, in a time frame set forth by the FIU Chief Information Security Officer, will result in disciplinary action as per FIU's ***Acceptable Use Policy***.

Definitions

Sensitive Information - 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.

Data Types:

FERPA – The Family Educational Rights and Privacy Act
Records that contain information directly related to a student and that are maintained by the University of Michigan or by a person acting for the university. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records.

Data Steward: University Registrar
Examples

- Grades
- Test Scores, assignments and class grades
- Student Financials, credit cards, bank accounts, wire transfers, payment history, financial aid/grants bills
- Disciplinary records
- Advising records
- Student tuitions bills
- Degree information
- Class schedule
- Student Transcripts

Laws/Regulations/Policies

U.S. Department of Education

GLBA – The Gramm–Leach–Bliley Act
Personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. Gramm Leach Bliley Act (GLBA) provisions govern this data type.

Data Steward: Director, Student Financial Services

Examples

- Student loan information
- Student financial aid and grant information
- Payment history

Laws/Regulations/Policies

Federal Trade Commission: Gramm-Leach-Bliley Act
Federal Standards for Safeguarding Customer Information

PCI – Payment Card Industry
Information related to credit, debit, or other payment cards. This data type is governed by the Payment Card Industry (PCI) Data Security Standards and overseen by the
FIU PCI Compliance Team.

Data Steward: Controller’s Office

Examples

- Credit/Debit Card numbers
- Cardholder name
- Credit/Debit Card expiration date
- Credit/Debit Card verification number
- Credit/Debit Card security code

Laws/Regulations/Policies

PCI Security Standards Council

HIPAA – The Health Insurance Portability and Accountability Act

Protected Health Information (PHI) is regulated by the Health Insurance Portability and Accountability Act (HIPAA). PHI is individually identifiable health information that relates to the

- Past, present, or future physical or mental health or condition of an individual.
- Provision of health care to the individual by a covered entity (for example, hospital or doctor).
- Past, present, or future payment for the provision of health care to the individual.

Researchers should be aware that health and medical information about research subjects may also be regulated by HIPAA.

Data Steward: HIPAA Compliance Team (COM, CCF, UCHS, DoIT, OGC, Compliance)

- Patient names, address, city, zip code, country, telephone / fax number
- Dates (except year) related to an individual, account / medical numbers, health plan beneficiary numbers
- PHI-related certificate / license numbers, license plate numbers, device ID's and serial numbers, email, URL's, IP addresses
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

Laws/Regulations/Policies

U.S. Dept of Health HIPAA website
Health and Human Services Information for Covered Entities

CUI – Controlled Unclassified Information
Controlled Unclassified Information (CUI), as defined by Executive Order 13556 (2010), is federal non-classified information that must be safeguarded by implementing a uniform set of requirements and information security controls directed at securing sensitive government information. CUI requirements do not apply directly to non-federal entities, but can flow down when FIU research projects receive, possess or create such information for or on behalf of the U.S. government under the terms of a contract, grant, or other agreement.

Data Steward: ORED

Examples

- CUI Registry Categories (https://www.archives.gov/cui/registry/category-list)
- CUI is a broad category that encompasses many different times of sensitive, but not classified, information.
- Personal identifiable information such as health documents, proprietary materials and information related to legal proceedings.
- Controlled technical information with military or space application

- Protected critical energy infrastructure information, including nuclear reactors and materials
- Export control information or materials

Even for those examples above, there must be specific contractual provisions that CUI requirements apply to information received, possessed, or created at FIU for or on behalf of the U.S government.

Laws/Regulations/Policies

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)

GDPR - General Data Protection Regulation
The General Data Protection Regulation (GDPR), which took effect May 25, 2018, affects organizations worldwide, including universities. The GDPR replaces the Data Protection Directive 95/46/ec as the primary law regulating how companies and organizations protect the personal data of people located in the European Union (EU).

Data Steward:

Examples:

Any information that relates to the identity of an individual located in the European Union

Different pieces of information, which collected together can lead to the identification of a particular person located in the European Union

Laws/Regulations/Policies:
General Data Protection Regulation (GDPR)

Export Controlled Research (ITAR, EAR)
Export Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism, or non-proliferation. The International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) govern this data type. Current law requires that this data be stored in the U.S and that only authorized U.S. persons be allowed access to it.

Data Steward:

Examples

- Chemical and biological agents and toxins
- Military electronics
- Documents detailing work on new formulas for explosives
- Military or defense articles and services
- Dual use technologies with both a commercial and military application
- Encryption technology
- Nuclear technology
- Space technology and satellites.

Laws/Regulations/Policies

U.S. Department of Commerce Export Controls

PII – Personal Identifiable Information

Personally Identifiable Information (PII) is a category of sensitive information that is associated with an individual person, such as an employee, student, or donor. PII should be accessed only on a strictly need-to-know basis and handled and stored with care.

PII is information that can be used to uniquely identify, contact, or locate a single person. Personal information that is "de-identified" (maintained in a way that does not allow association with a specific person) is not considered sensitive.

- Name,
- Address
- date of birth
- telephone numbers
- maiden name
- ethnicity
- gender
- websites visited
- bank and credit/debit card numbers
- IP address in conjunction with other PII.
- photographic images
- fingerprints
- driver's license number
- place of birth
- weight
- employment information
- education information
- financial information.

FLORIDA
INTERNATIONAL
UNIVERSITY

SCOPE

This guideline applies to all FIU's faculty, staff, students and any other external individuals (e.g.) contractors, vendors and consultants) contracted into a business agreement with FIU.
Florida International University, IT Security Office, is responsible for the oversite and, where applicable, the enforcement of any regulations that may apply to a data class.

REASON FOR STANDARD

This standard informs all applicable FIU faculty, staff, and 3rd party users that have access to institutional data what is the accepted method of use, classification, and associated controls, as per the university's policies and standards, and state and federal laws and regulations.

ROLES AND RESPONSIBILITIES

As per FIU "Data Stewardship" procedure (1930.020a), FIU has established a procedure for dealing with "Highly Sensitive Data" and the need for higher level of security when data is given this classification. Departments that handle "Highly Sensitive Data" are directly vested in the storage and possible creation of the data; as such, a department is ultimately responsible for the security of its data. All FIU employees, students and authorized users of the IT data resources are considered **"Data Stewards"**.
Departments storing data classified as "Level 3 – Confidential Data" must designate a **"Data Owner"** for their department and this must be documented in the "List of Data Stewards". This list shall be maintained by the IT Security Office. The Data Owner may be a division head, director, manager or equivalent. The Data Owner is responsible for the department's use of the data and must enforce DoIT security controls listed in this policy.

RELATED RESOURCES

FIU Approved Services and Data Classification

CONTACTS

Division of Information Technology

FLORIDA
INTERNATIONAL
UNIVERSITY

IT Security Office
11200 SW 8 ST, PC534
Miami, FL 33199
Security@fiu.edu
305-348-1366

HISTORY

List initial effective date, revision dates, and/or review date.

Initial Effective Date: April 24, 2024
Review Dates (*review performed, no updates*): April 24, 2024
Revision Dates (*updates made to document*): April 24, 2024