



Data Classification Standard

INITIAL EFFECTIVE DATE: October 30, 2021	LAST REVISION DATE: February 26, 2026	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT Information Security Office
--	---	--

PURPOSE

FIU’s Data stored in electronic 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.

SCOPE AND AUTHORITY

This standard applies to all FIU faculty, staff, students and any other external individuals (e.g. contractors, vendors and consultants) who contracted into a business agreement with FIU.

Florida International University’s IT Security Office is responsible for the oversight and, where applicable, the enforcement of any regulations that may apply to a data classification.

ROLES AND RESPONSIBILITIES

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 Owners”. 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.

Information previously categorized as “Highly Sensitive Data”, will now be classified as level 3, Confidential Data, unless an exception is made by the IT Security Officer. Further information on the “Highly Sensitive Data” can be found in [FIU’s Data Stewardship](#) policy.



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**.

CLASSIFICATION AND SECURITY REQUIREMENTS

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.

Data classification needs to be considered when sharing information with [Artificial Intelligence](#) models and storing on any media including [removable media](#). No level 2 or 3 data should be submitted to publicly available AI models as stated in the [AI guidelines](#).

Level 3 – 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.

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

Regulations that fall under this category include FERPA, GLBA, PCI, HIPAA, CUI and GDPR.

Level 3, Confidential Data Examples:

- 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
- Student records, Exam records, and Financial data

Level 2 – 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.

Level 2, Internal/Private Data Examples

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- Unpublished research data (with data owner's approval)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

Level 1 – 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.

Level 1, Public Data Examples:

- Job postings
- University directory Information
- Information in the public domain
- Publicly available campus maps
- Published research publications and data
- 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.

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 Florida International University or by a person acting for the university. The Family Educational Rights and Privacy Act 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 for FERPA:

- ✓ [U.S. Department of Education](#)
- ✓ [FIU-108 Access to Student Education Records](#)
- ✓ [FIU-2507 Examinations and Assessments](#)



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 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 for GLBA:

- ✓ [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 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 for PCI:

- ✓ [PCI Security Standards Council](#)
- ✓ [Payment Card Processing Policy \(1110.025\)](#)

HIPAA – The Health Insurance Portability and Accountability Act

Protected Health Information (PHI) is regulated by the Health Insurance Portability and Accountability Act. 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: Assigned HIPAA liaison

Examples:

- 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 for HIPAA:

- ✓ [U.S. Dept of Health HIPAA website](#)
- ✓ [Health and Human Services Information for Covered Entities](#)
- ✓ [HIPPA Privacy and Security](#)

CUI – *Controlled Unclassified Information*

Controlled Unclassified Information, 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 for CUI:

- ✓ [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 \(NIST SP 800-171A\)](#)
- ✓ [Protection of Controlled Unclassified Information \(CUI\) \(1930.001\)](#)

GDPR - General Data Protection Regulation

The General Data Protection Regulation, 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: GDPR Committee

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 for GDPR:

- ✓ [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: Compliance and ORED

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 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.

Data Steward: Multiple areas

Examples

- 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



RESOURCES

[Artificial Intelligence](#)
[Artificial Intelligence Guidelines](#)
[Data Stewardship Policy](#)
[Removable Media Standard](#)

CONTACTS

Florida International University - Division of Information Technology
IT Security Office
Security@fiu.edu

HISTORY

Initial Effective Date: October 30, 2021
Review Dates (review performed, no updates): N/A
Revision Dates (updates made to document):
2/26/2026 (updated overall document)
3/20/2026 (added link to Removable Media Standard)