

Florida State University

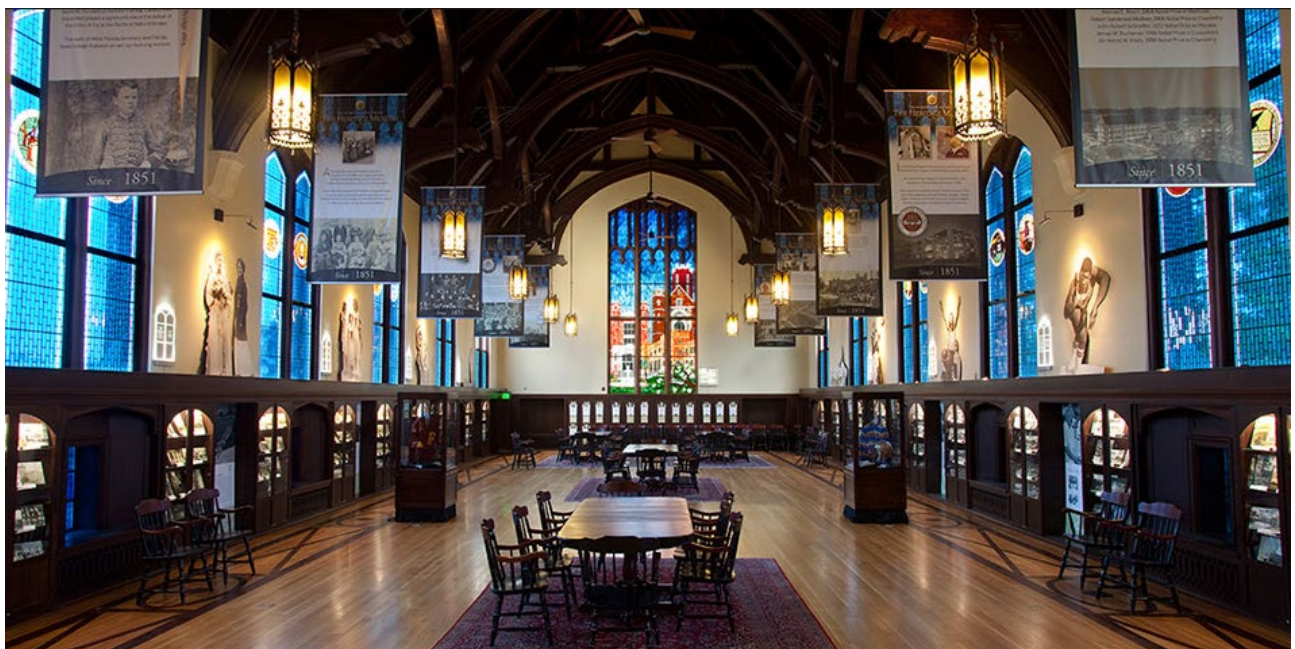
INFORMATION RISK MANAGEMENT PROGRAM

Information Classification Guidelines

Information Security & Privacy Office

May 1, 2020

Version 2.14



Information Classification Guidelines

Purpose

Florida State University (FSU) takes seriously its obligation to respect and protect the privacy of its students, alumni, faculty and staff, as well as to safeguard the confidentiality of information important to the University's academic and research mission.

By classifying information at FSU, we take the first step toward identifying information that should be protected based on University policies and applicable state and federal laws. Understanding the classification and value of University information provides the intelligence necessary for faculty, staff and administration to determine the most cost effective and appropriate level of protection as part of a risk-based approach to security and privacy controls implementation.

Information classification supports:

- Compliance with legal and regulation requirements;
- Mapping information protection levels with organizational needs;
- Efficient budgeting by implementing controls where they are needed the most;
- Reducing risks associated with the unauthorized access and disclosure of University protected or private information.

All University information, regardless of the format or medium of the record (paper, electronic information/voice/video/image, microfilm, etc.), should be classified into one of three sensitivity levels categories:

Level 1 - Protected
Level 2 - Private
Level 3- Public

Reclassification




Campus units should periodically reevaluate information classifications to ensure the delegated classification is still appropriate. Changes to laws and rules, contractual obligations, or how certain information is used can result in modification to the information's value to the University and its classification. Appendix B contains University and other resources to assist in this process.

Direct-Support Organizations

Groups defined as Direct-Support Organizations (DSO) under Florida Statute 1004.28 should consult their legal counsel for classification assistance. DSO's are considered a Florida corporation not for profit incorporated under the provisions of chapter 617 and are exempt from the Florida Statute 119 Public Records requirements. Information items classified as "Private" for FSU should have elevated privacy status for a DSO.

Levels of Data Security at FSU

See Appendix A for data classification examples for each level and Appendix B for links to classification resources.

Level 1 - Protected 	Level 2 - Private 	Level 3 – Public 
<p>Criteria used to classify FSU information as “Level 1 - Protected” include:</p> <ol style="list-style-type: none"> 1) Any information that could, if exposed, create civil or criminal penalties, reputational damage, loss of protected intellectual property. 2) Select information protected by law or contractual obligation including: <ul style="list-style-type: none"> • Student Information (FERPA) • Personal Health Information (PHI) • Credit Card Information • Student Financial Aid Information (GLBA) • Certain types of Research • Social Security Numbers • Driver’s License Numbers • Human Subject Research 3) University information exempt from public disclosure under the provisions of Florida Statute Chapter 119, Public Records. 	<p>Criteria used to classify FSU information as “Level 2 – Private” include:</p> <ol style="list-style-type: none"> 1) Information used in the normal course of university business but not normally released to the public unless subject to a public records request. 2) Information whose access must be guarded due to proprietary, ethical, or privacy considerations. 3) Research work in progress. 	<p>Criteria used to classify FSU information as “Level 3 - Public” include:</p> <ol style="list-style-type: none"> 1) Information intended to be readily obtainable by the public.

APPENDIX A – DATA CLASSIFICATION EXAMPLES

The following are select examples by type to facilitate uniformity in the classification process. Use the criteria defined in each category for information items not found within these lists. Engage the Information Security and Privacy Office for assistance with classification issues.

Note: Changes in legislation or contracts may result in adjustments to classification levels for the examples listed below. It is the responsibility of the information owner to engage in a periodic review of their information resources to maintain the proper classification level(s).

Examples of Level 1 - Protected information

- ✓ An individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following information elements (F.S. 501.171 and F.S. 119.071):
 - Social security number;
 - Driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
 - Financial account number or credit or debit card number, in combination with any required security code, access, code, or password that is necessary to permit access to an individual's financial account;
 - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
 - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or
 - Any other information from or about an individual that could be used to personally identify that person.
- ✓ Personal information on FSUPD law enforcement officers, their families, and other protected employees as defined by (F.S. 119.071)
- ✓ Information associated with a campus emergency response of the university. "Campus emergency response" is defined as the university's response to or plan for responding to an act of terrorism or other public safety crisis or emergency. (F.S. 1004.0962)
- ✓ Records held by the university which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, if the disclosure of such records would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of information assets. (F.S. 1004.055)
- ✓ Information relating to the security of the university's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; those portions of risk assessments, evaluations, audits, and other reports of the university's or institution's information technology security program for its data, information, and information technology resources which are held by the university or institution, if the disclosure of such records would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction

Continued Examples of Level 1 - Protected information

- of university information assets. (F.S. 1004.055)
- ✓ Computer system passwords and security codes (F.S. 501.171)
- ✓ Employee records designated as "Limited-Access Records" by the FSU Board of Trustees (F.S. 1012.91)
- ✓ Vulnerability/security/configuration information related to a campus information system/network or physical security system (F.S. 1004.055)
- ✓ Information processing software obtained under licensing agreement prohibiting its disclosure and where software is a trade secret (F.S. 1004.055)
- ✓ Those portions of risk assessments, evaluations, audits, and other reports of the university's or institution's information technology security program for its data, information, and information technology resources which are held by the university or institution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:
 1. Data or information, whether physical or virtual; or
 2. Information technology resources, which include:
 - a. Information relating to the security of the university's or institution's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or
 - b. Security information, whether physical or virtual, which relates to the university's or institution's existing or proposed information technology systems. (F.S. 1004.055)
- ✓ Credit card number/ Card Verification Value (PCI DSS)
- ✓ Debit card number (PCI DSS)
- ✓ Student passport numbers (FERPA)
- ✓ Sealed bids, proposals, or replies pursuant to competitive solicitation (F.S. 119.071)
- ✓ Vendor Employer Identification Number
- ✓ Vendor bank account and routing numbers
- ✓ Electronically stored biometric information (F.S. 119.071):
 - Any record of friction ridge detail;
 - Fingerprints;
 - Palm prints; and
 - Footprints.
- ✓ Medical records, personally identifiable medical information, and all information designated as "Protected Health Information" (HIPAA, FERPA)
- ✓ Research datasets with sensitive and/or private information provided under special agreement with a federal, state, or private entity (OMB Circular A-110, Contract)
- ✓ Research information related to sponsorship, funding, human subject, etc.
- ✓ Research information and results designated in contracts as Controlled Unclassified Information (CUI)
- ✓ Research datasets subject to International Traffic in Arms Regulations or Export Administration Regulation restrictions (ITAR, EAR)
- ✓ Unpublished grant proposals and unpublished research information (Contract, Laws)
- ✓ Unpublished manuscripts and correspondence (Contract, Laws)
- ✓ All FSU attorney-client communications and University attorney work product (F.S. 119.071)
- ✓ Non-public donor and alumni information

- ✓ Information concerning human research subjects (Public Law 93-348)
- ✓ Information obtained by FSU from third parties under non-disclosure agreements or any other contract that designates third party information as confidential (Contracts, Laws)
- ✓ Covered Defense Information as defined in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008 - Compliance with Safeguarding Covered Defense Information Controls, and Sub Contract Clause Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting. Includes information identified as Controlled Technical Information (CTI) and Controlled Unclassified Information (CUI).
- ✓ Information and systems controlled under the Federal Acquisition Regulations (FAR) 52.204-21 contract clause.
- ✓ Information and systems designated in contracts and grants as Federal Information Security Modernization Act (FISMA) Low, FISMA Moderate or FISMA High.
- ✓ Select data items of a student's educational record not classified as "Directory information" by the university, the educational record of a student who files a written request to block the release of their "Directory Information," or as stipulated under the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). Education records are records that are directly related to a student and that are maintained by the university or a party acting for or on behalf of the university. FERPA provisions extend to currently or formerly enrolled student's educational records, regardless of their age or parental-dependency status. However, FERPA does not extend to deceased students or students who have applied to FSU but have not attended any classes.

Select examples of a student's educational record considered "Non-Directory" by the university at the time of publishing these guidelines include, but are not limited to:

- FSUID
- Student email address
- FSUSN
- Coursework
- Transcripts, defined as any cumulative listing of a student's grades
- Graded work, grade book, etc.
- Student and Exchange Visitor Information System (SEVIS) Number

(>>Refer to the FSU Registrars website for a current list of data items declared as "Directory Information" by the university as the list is subject to change.)

Examples of **Level 2 – Private** information

- ✓ E-mail correspondence
- ✓ Budgetary, departmental, or University planning information
- ✓ Purchasing – Responses to solicitation requests
- ✓ Campus attorney-client communications
- ✓ University's investment information
- ✓ Employee's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following information elements (Students in work study or graduate assistant positions retain FERPA protections)
 - Date of birth
 - Home address

- Personal telephone numbers
- Personal email address
- Employee evaluations
- FDLE/FBI employment background investigations
- Race and ethnicity
- Gender
- Marital status
- Emergency Contact Information
- ✓ Personal notes on students held by faculty/staff that are not considered part of a student's official record
- ✓ Library transactions (e.g., circulation, acquisitions)
- ✓ Private funding information
- ✓ Course evaluations
- ✓ Academic course exams
- ✓ De-Identified information used in research
- ✓ Information from research germane to intellectual property not categorized as "Protected"

Examples of Level 2 – Private information

- ✓ Restricted-Use Contractual Information
- ✓ Other information specifically designated as Private by the university
- ✓ Trade secrets or intellectual property such as research activities

Examples of Level 3 – Public information

- ✓ Student information elements classified as Directory information by the University Registrar (Exclusion applies for students who file a "Request to Prevent Release or Publication of Directory Information" with the Office of Admissions and Records who retain FERPA protections over selected Directory Information) (Refer to the FSU Registrars site for a current list of FERPA directory information.)
 - Name
 - Date and place of birth
 - Local address
 - Permanent address
 - Telephone number (if listed)
 - Classification
 - Major
 - Participation in official University activities and sports
 - Weight and height of athletic team members
 - Dates of attendance
 - Degrees, honors, and awards received
 - Most recently attended educational institution
 - Digitized FSUCard photo
 - EMPLID
- ✓ Financial information on public sponsored projects
- ✓ General information public websites
- ✓ Official statements and press releases

- ✓ Course information/materials
- ✓ Research information that has been de-identified in accordance with applicable rules
- ✓ Published research
- ✓ Public-Use information
- ✓ Directories
- ✓ Maps
- ✓ Syllabi
- ✓ Faculty/Staff information not protected under F.S. 119.071 including:
 - EMPLID
 - FSUSN
 - Name
 - Email address
 - Title
 - Department
 - Listed telephone number(s)

APPENDIX B – DATA CLASSIFICATION RESOURCES

Student Records - Family Educational Rights and Privacy Act (FERPA)

FSU Registrar FERPA Information Website

<https://registrar.fsu.edu/records/ferpa/>

U.S. Department of Education FERPA Website:

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Student Financial Records - Gramm-Leach-Bliley Act (GLBA)

Gramm-Leach-Bliley Act (GLBA)

<http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>

Health Records - Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) - Privacy Rule

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/>

Health Insurance Portability and Accountability Act (HIPAA) – Security Rule

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>

HITECH Act Enforcement Interim Final Rule

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>

Research Records

FSU Office of Research – Research Compliance Resources

<http://www.research.fsu.edu/researchcompliance/>

FSU Office of Research - Human Subjects Committee

<http://www.research.fsu.edu/humansubjects/>

Controlled Unclassified Information (CUI)

<https://www.archives.gov/cui>

The International Traffic in Arms Regulations (ITAR)

https://www.pmdtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing

Export Administration Regulation (EAR)

<http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>

Federal Policy for the Protection of Human Research Subjects (Common Rule)

<http://www.hhs.gov/ohrp/humansubjects/index.html>

Research Involving Human Subjects – (NIH)

<http://grants.nih.gov/grants/policy/hs/>

The Belmont Report (Human Subjects of Biomedical and Behavioral Research)

<http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>

OMB Circular A-110

<https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-110.pdf>

National Institutes of Health – Grants Policy and Guidance

<https://grants.nih.gov/grants/policy/policy.htm>

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls

http://farsite.hill.af.mil/reghtml/regsfar2afmcfars/fardfars/dfars/dfars252_000.htm#P842_4447

APPENDIX B – DATA CLASSIFICATION RESOURCES (CONTINUED)

National Institute of Standards and Technology Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>

Credit/Debit Card Records

Payment Card Industry – Data Security Standards

<https://studentbusiness.fsu.edu/about/merchant-services>

University Payment Cards Policy 4-OP-D-2-G

<https://policies.vpfa.fsu.edu/policies-and-procedures/financial/payment-cards-policy>

Employee Records

The Genetic Information Nondiscrimination Act (GINA)

<https://www.eeoc.gov/laws/statutes/gina.cfm>

Websites

Children's Online Privacy Protection Rule (COPPA)

<http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

FBI Criminal Records

Criminal Justice Information Systems (CJIS)

<http://www.fbi.gov/about-us/cjis>