FLORIDA STATE UNIVERSITY
INFORMATION SECURITY & PRIVACY

University Data Classification Guidelines

Florida State University
Information Security and Privacy Office (ISPO)
2014

Data Classification Guidelines

Purpose

Florida State University 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 data at Florida State University, we take the first step toward identifying data that should be protected based on University policies and applicable state and federal laws. Understanding the classification and value of University data 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.

Data classification supports:

- Compliance with legal and regulation requirements;
- Mapping data 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 data.

All University data, regardless of the format or medium of the record (paper, electronic data/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 data classifications to ensure the delegated classification is still appropriate. Changes to laws and rules, contractual obligations, or how certain data is used can result in modification to the data’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. Data items classified as “Private” for FSU should have elevated privacy status for a DSO.

Classification Description: Level 1 – Protected

The **Protected** classification encompasses data deemed confidential under federal or state law or rules, FSU contractual obligations, or privacy considerations such as the combination of names with respective Social Security Numbers. Protected data requires the highest level of safeguarding protection.

Criteria used to classify FSU information as "**Level 1 - Protected**" include:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of Florida Statutes 119.071.

b) Severe or catastrophic risk - Information whose unauthorized access or modification will result in substantial reputational, financial, or research impairment to FSU and its data stakeholders.

c) Limited use - Information intended solely for use within FSU and limited to those with a "business need-to know."

d) Legal Obligations - Information for which laws, rules, regulations, or contractual obligations dictate specific security and privacy controls to safeguard data, restrict access, or limit transmission (See Appendix B for examples of legal or contractual obligations for select University data).

See Appendix A for examples of Level 1 – Protected data

Classification Description Level 2 - Private

The **Private** classification encompasses data for which the unauthorized disclosure may have moderate adverse effects on the university's reputation, resources, services, or individuals. This is the default classification, and should be assumed when there is no information indicating that data should be classified as Public or Protected.

Criteria used to classify FSU information as "**Level 2 – Private**" include:

a) Information which is not specifically protected by legal or contractual mandates but for which unauthorized access or modification could cause financial loss, damage to FSU's reputation, violate an individual's privacy rights, or make legal action necessary.

b) Limited use – Private information intended for internal FSU use or shared with select outside entities to facilitate research or business functions.

Note: Under Florida Statute Chapter 119, Public Records, data classified Private may be subject to personal inspection and copying.

See Appendix A for examples of Level 2 – Private data

Classification Description Level 3 - Public

The **Public** classification encompasses data for which disclosure to the public poses negligible or no risk to the University's reputation, resources, services, or individuals.

Criteria used to classify FSU information as “**Level 3 - Public**” include:

a) Information designated as publically available and/or intended to be provided to the public.

b) Disclosure of this information does not expose FSU to financial loss or jeopardize the security of information assets or the physical security of those associated with the University.

See Appendix A for examples of Level 3 – Public data

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 data 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 data 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)*
- ✓ *Computer system passwords and security codes (F.S. 501.171)*
- ✓ *Faculty and Staff personnel records designated as "Limited-Access Records" by the FSU Board of Trustees (F.S. 1021.91)*
- ✓ *Vulnerability/security/configuration information related to a campus data system/network or physical security system (F.S. 119.071)*
- ✓ *Data processing software obtained under licensing agreement prohibiting its disclosure and where software is a trade secret (F.S. 119.071)*
- ✓ *Building plans or blueprints (F.S. 199.071)*
- ✓ *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)*
- ✓ *Medical records, personally identifiable medical information, and all information designated as "Protected Health Information" (HIPAA, FERPA)*

Examples of **Level 1 - Protected** information (continued)

- *Research information related to sponsorship, funding, human subject, etc.*
- *Research datasets with sensitive and/or private data provided under special agreement with a federal, state, or private entity (OMB Circular A-110, Contract)*
- *Research datasets subject to International Traffic in Arms Regulations or Export Administration Regulation restrictions (ITAR, EAR)*
- *Unpublished grant proposals and unpublished research data (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*
- *Data 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)*
- *Select student record data items (FERPA)*
    - *EMPLID*
    - *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*

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 data elements (Students in work study or graduate assistant positions retain FERPA protections)*
    - *EMPLID*
    - *FSUSN*
    - *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

APPENDIX A – DATA CLASSIFICATION EXAMPLES (CONTINUED)

Examples of **Level 2 – Private** information

- ✓ Academic course exams
- ✓ *De-Identified data used in research*
- ✓ *Data from research germane to intellectual property that is not categorized as "Protected"*
- ✓ *Restricted-Use Contractual Data*
- ✓ *Other data specifically designated as Private by the university*
- ✓ *Trade secrets or intellectual property such as research activities*

Examples of **Level 3 – Public** information

- ✓ *Student data 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)*
  - ○ *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*
- ✓ *Financial data on public sponsored projects*
- ✓ *General information public websites*
- ✓ *Official statements and press releases*
- ✓ *Course information/materials*
- ✓ *Research data that has been de-identified in accordance with applicable rules*
- ✓ *Published research*
- ✓ *Public-Use data*
- ✓ *Directories*
- ✓ *Maps*
- ✓ *Syllabi*
- ✓ *Select Faculty/Staff information including:*
  - ○ *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
http://registrar.fsu.edu/ferpa/apdefault.htm

FSU Registrar FERPA FAQ
http://registrar.fsu.edu/ferpa/faq.htm#Communicating01

FSU Registrar Faculty & Staff Reference Sheet
http://registrar.fsu.edu/ferpa/files/ferpa_faculty_staff.doc

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/

The International Traffic in Arms Regulations (ITAR)
http://www.pmddtc.state.gov/regulations_laws/itar.html

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
http://www.whitehouse.gov/omb/circulars_a110

National Institutes of Health – Grants Policy and Guidance
https://grants.nih.gov/grants/policy/policy.htm

APPENDIX B – DATA CLASSIFICATION RESOURCES (CONTINUED)

Credit/Debit Card Records

Payment Card Industry – Data Security Standards

http://controller.vpfa.fsu.edu/Student-Financial-Services/SFS-for-Departments/PCI-Training

University Payment Card Policy OP—D-2-G

http://policies.vpfa.fsu.edu/controller/2d-4.html

Employee Records

The Genetic Information Nondiscrimination Act (GINA)

http://ghr.nlm.nih.gov/spotlight=thegeneticinformationnondiscriminationactgina

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