Data Classification Standards
University of Alaska

Table of Contents

Section 1. Background

1.1. Context for Data Classification Standards

The University of Alaska (UA) generates, acquires, and maintains a large number of electronic records. In addition, UA often enters into relationships with third parties who maintain electronic records and information associated with these relationships. UA, as well as its affiliates, are often legally required to limit access to, distribution of, and/or disclosure of electronic records and information.

Proper protection of data is determined by a combination of compliance requirements mandated by Board of Regents policy, State and Federal statutes and regulations, institutional risk management policies, and accepted best practices. The approach taken at UA is to first adopt a classification scheme for all data and then establish appropriate measures to protect it. A separate document will recommend best practices and measures to provide appropriate protection for each class of data.

1.2. Purpose

Data classification standards help the people who own and maintain information resources and systems to determine the sensitivity of the data within those systems. These standards should be read and applied in conjunction with the UA Information Systems Security Policy (TBD) and the UA Minimum Computer Security Standards (TBD) (http://www.alaska.edu/it/security/standards). These three documents are designed to prevent the following:

- Unauthorized internal access to electronic information
- Unauthorized external access to electronic information
- Illegal or otherwise inappropriate use of UA electronic information
- Loss, corruption, or theft of UA electronic information

1.3. Applicability

This classification standard applies to all data associated with UA business; to any other data caches located at any UA entity and covered by statutory or regulatory compliance requirements; and to data caches on the information systems of UA affiliates. Data associated with UA-hosted research that represent significant intellectual property interests are subject to this standard and may be subject to other specific protective requirements.

Questions about the applicability of this standard can be forwarded to the UA Chief Information Security Officer for review by the Compliance Assurance and System Security Council (CASS).

1.4. Audience

The target audience for these standards includes all individuals who have access to and use UA information systems and data, particularly UA systems owners and designated data custodians who have special responsibilities under the standards (see Appendix A, Glossary).

Section 2. Data Classification and Examples

The nature of any particular data set largely determines what measures and operational practices need to be applied to protect it. To help clarify the specific minimum requirements for UA data security, three classes of data are defined. The people who are accountable for protecting the data must understand and inventory their data assets according to these categories.

- **Restricted Data:** Data classified as restricted maybe subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information is considered private and must be guarded from disclosure. Unauthorized

exposure of this information could contribute to ID theft or financial fraud and violate State and Federal law. Unauthorized disclosure of restricted data could adversely affect the university or the interests of individuals and organizations associated with the university.

- **Internal Use Data:** This class encompasses information that is generally not available to parties outside the University of Alaska community such as non-directory listings, minutes from non-confidential meetings, and internal websites. Public disclosure of this information would cause minimal trouble or embarrassment to the institution. The university may have a duty to make this data available on demand under the Alaska Public Record Act (AS 40.25.110).

- **Public Data:** Public data is data published for public use or has been approved for general access by the appropriate UA authority.

In most cases categorizing the data will be obvious. When in doubt about how a particular data element or data set is classified, data custodians should use caution by defaulting to the higher class of the choices involved. In other words, it is better to err on the side of privacy and security protection until clarification is obtained.

The source data used to produce important reports, such as UA financial records, are treated as restricted or internal use even though the reports created from them are treated as public information. Data classification questions may be forwarded to the UA Chief Information Security Officer for review by the Compliance Assurance Systems Security Council (CASS).

Table 1 clarifies the nature of each data category and provides criteria for determining which classification is appropriate for a particular set of data. When using this table, a positive response for the most restrictive (highest risk) category in any row is sufficient to place that set of data into that category.

Table 1. Data Classification Categories

Class	Restricted	Internal Use	Public
Legal Requirements	Protection of data is required by law or best practices	UA has best practice (due care) reasons to protect data	Data approved for general access by appropriate UA authority
Risk level	**High**	**Medium**	**Low**
Consequences of Exposure	The University's reputation is tarnished by public reports of its failures to protect restricted records of students, employees, clients, or research. Such failure may subject the University to litigation.	Data is disclosed unnecessarily or in an untimely fashion, which causes harm to UA business interests or to the personal interests of an individual.	Confusion is caused by corrupted information about enrollment and tuition that is displayed on the official UA web site
Examples of Specific Data	● HIPAA[1]- Protected data when associated with a health records ● FERPA[2]-individual student records ● Research – EAR, export controls, ITAR, TCP, safeguarding confidential information[3]	● Employee Internet usage ● Specific technical security measures ● UA employee business-related email (including student employees, but only their work-related email) ● Location of assets	● Campus promotional material ● Annual reports ● Press statements ● Job titles ● Job descriptions ● Employee work phone numbers (with special exceptions)

	● Information required to be protected by contract ● Human subjects identifiable research data ● Trade secrets, intellectual property and/or proprietary research ● Attorney/client privileged records ● Payment Card Industry[4] (PCI) ● University banking records ● Restricted police records (e.g., victim information, juvenile records) ● Computer account passwords ● Gramm-Leach-Bliley[5] (GLB) ● Certain affirmative action related data[6] ● Alaska Personal Information Protection Act[7] ● Library records confidentiality AS40.25.140	● Faculty promotion, tenure, evaluations ● Supporting documents for UA business functions ● Public research AS 14.40.453 ● Supporting documents for UA business functions ● Aggregate human subjects research data ● Animal research ● Proposal records	● University of Alaska business records ● Employee work locations (with special exceptions) ● Employee email addresses (with special exceptions)

See Appendix B for examples of restricted data

Data classification and categories may change as laws and compliance regulations are modified or added.

[1]For more information on the Health Insurance Portability and Accountability Act (HIPAA) see:
http://www.alaska.edu/hr/benefits/open_enrollment/hipaa_privacy.pdf
http://www.uaf.edu/chc/privacy.html
http://www.uaa.alaska.edu/facultyservices/upload/HANDBOOK%20Chapter%20VI.dot.

[2]All written information related to a specific student that is not considered directory information or is not contained in university police records is considered restricted. In addition to the examples listed in Table 1, any written communications about a student, including email to, from, and about a student, audio/video tapes of a student engaged in class-related functions, etc., unless the student has signed a written release, is considered restricted. For more information on the Family Educational Rights Privacy Act (FERPA), see:
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
http://www.alaska.edu/studentservices/ferpa/
http://www.uaa.alaska.edu/records/app/ferpa.cfm.

[3]For more information on UA research, see:
http://www.uaf.edu/ori/Policies/Confidential_Information.pdf
http://www.uaf.edu/ori/Export_Management.htm

[4]The credit card industry, calling itself the Payment Card Industry (PCI), has implemented the Cardholder Information Security Program (CISP) to protect its customers, and CISP compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The PCI standard is designed to safeguard sensitive data for all card brands. This standard is a collaborative result between Visa, MasterCard, and other card companies, and is designed to create common, industry-wide security requirements. For more information on the Payment Card Industry (PCI), see:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
http://usa.visa.com/merchants/risk_management/cisp_overview.html

[5]"The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB Act), includes privacy provisions to protect consumer information held by financial institutions. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law. The Safeguards Rule of the GLB Act requires financial institutions to have a security plan to protect confidentiality and integrity of personal information. Privacy notices explaining an institution's information-sharing practices must also be provided. As of May 23, 2003, colleges and universities must be in compliance with provisions of the GLB Act that relate to the Safeguards Rule. Colleges and universities that already comply with the Family Educational Rights and Privacy Act (FERPA) will be deemed to be in compliance with FTC privacy rules under the GLB Act." For more information on the Gramm Leach Bliley (GLB), see:
http://connect.educause.edu/term_view/GLB+Act (From which the foregoing except comes.)
http://www.american.edu/counsel/pages/pdf/gramm_fact_sheet.pdf
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106

[6]For more information on UA affirmative action policy, see:
http://www.alaska.edu/bor/policy/4p/p04-02.html

[7]For more information on Alaska's Personal Information Protection Act (HB 65, which became law on June 13, 2008), see:
http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=HB0065Z&session=25

Appendix A. Glossary

Confidentiality: Confidentiality is an attribute of information. Confidential information is sensitive, contractually protected, or information whose loss, corruption, or unauthorized disclosure could be harmful or prejudicial.

Data Custodian: As defined in the UA Information Systems Security Policy, data custodians are individuals who have been officially designated as being accountable for protecting the confidentiality of specific data that is transmitted, used, or stored on a system or systems within a department, college, school, or administrative unit of the UA and certain affiliated organizations.

Internal Use Data: this information is generally not available to parties outside of the University of Alaska and includes such things as non-directory listings, minutes from non-confidential meetings, and the internal (intranet) websites. Public disclosure of this information would cause minimal trouble or embarrassment to the institution. The university may have a duty to make this data available on demand under the Alaska Public Record Act (AS 40.25.110).

Personally Identifiable Information: Personally identifiable information is defined as data or other information that is tied to or which otherwise identifies an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known.

Personal information includes, but is not limited to, information regarding a person's home or other personal address, social security number, driver's license, marital status, financial information, credit card numbers, bank account numbers, parental status, sexual orientation, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, home or other personal phone numbers, non-university address, employee number, personnel or student records, and information related to the UA affirmative action policy.

Privacy: Privacy refers to an individual right to be left alone, to withdraw from the influences of his or her environment, or to be secluded, not annoyed, and not intruded upon. It includes a person's right to be protected against the misuse or abuse of something legally owned by an him or her, or something that is normally considered by society to be his or her property.

Public Data: Public data is the data that is published for public use or has been approved for general access by the appropriate UA authority.

Record: Recorded information—regardless of medium or characteristics, whether made or received by the University—that is evidence of its operations and has value requiring its retention for a specific period of time constitutes a record.

> [State of Alaska Records Definition – AS sect 40.21.150 (6)] "Record means any document, paper, book, letter, drawing, map, plat, photo, photographic file, motion picture film, microfilm, microphotograph, exhibit, magnetic or paper tape, punched card, electronic record, or other document of any other material, regardless of physical form or characteristic, developed or received under law or in connection with the transaction of official business and preserved or appropriate for preservation by an agency or a political subdivision, as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the state or political subdivision or because of the informational value in them; the term does not include library and museum material developed or acquired and preserved solely for reference, historical or exhibitions

purposes, extra copies of documents preserved solely for convenience of reference, or stocks of publications and processed documents."

Restricted Data: Data classified as restricted maybe subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information is considered private and must be guarded from disclosure. Unauthorized exposure of this information could contribute to ID theft, financial fraud, and violate State and Federal laws. Unauthorized disclosure of this data could adversely affect the university or the interests of individuals and organizations associated with the university.

Security: Security is an attribute of information systems practices that includes specific policy-based, procedural, and technical mechanisms and assurances for protecting the confidentially and integrity of information, the availability and functionality of critical services, and the confidentiality of sensitive information.

Sensitive Information: Information is generally considered sensitive when it requires access controls and other control measures to meet legal, policy, and/or ethical requirements.

System: Any network, computer, software package, or other entity for which there can be security concerns would constitute a system.

System(s) Owners: As defined in the UA Information Systems Security Policy, systems(s) owners are individuals within the UA community who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that support UA business, client services, educational, or research activities that are associated with or hosted by the University.

Users: Any individual that has been granted access and privileges to UA computing and network services, applications, resources, and information.

Appendix B. Examples of Restricted Data

Institutional Data covered by this document may include but are not limited to the following examples of restricted data:

HIPAA (Health Insurance Portability and Accountability Act) – Protected Health Information

- Patient names
- Street Address, city county, zip code
- Dates (except year) for dates related to an individual
- Telephone/facsimile numbers
- E-mail, URLs, & IP numbers
- Social security numbers
- Account/Medical records numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identification's and serial numbers
- Device identification numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

FERPA (Family Educational Rights Privacy Act) – Student Records

- Grades/Transcripts
- Class lists or enrollment information
- Student Financial Services information
- Athletics or department recruiting information
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfer Information
- Payment History
- Financial Aid/Grant information /loans
- Student Tuition Bills

GLB (Gramm-Leach-Bliley) – Protects confidentiality and integrity of personal information

- Employee financial account information
- Student financial account information
- Individual financial information
- Business partner and vendor financial account information

Alaska Personal Information Protection Act – Protects any form of information on an individual that consists of a combination of that individual's name with one or more of the following:

- Social security number
- Driver's license number
- State identification number
- Passport number
- Credit or debit card number
- Bank account number
- An account that only be accessed with a personal code
- Passwords, personal identification numbers, or other access codes for financial accounts
- Medical information
- Insurance policy number

Appendix C. Bibliography

Alaska State Legislature. Bill Text 25 Legislature: House Bill 65 Personal Information Protection Act. http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=HB0065Z&session=25 (June 2, 2008)

American University. Gramm Leach Bliley Fact Sheet. http://www.american.edu/counsel/pages/pdf/gramm_fact_sheet.pdf (June 10, 2008).

EDUCAUSE. Gramm-Leach-Bliley Act of 1999 (GLB ACT). http://connect.educause.edu/term_view/GLB+Act (June 10, 2008).

Federal Trade Commission. Privacy Initiatives: The Gramm-Leach Bliley Act. http://www.ftc.gov/privacy/privacyinitiatives/glbact.html (June 12, 2008).

Financial Services Modernization Act of 1999 ("Gramm-Leach-Bliley Act"). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106. (October 22, 2008).

Open Source Web Application Security Project (OWASP) standards for secure coding. (http://www.owasp.org/index.php/Main_Page (July 8, 2008).

Security Standards Council. About the PCI Data Security Standard. https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (May 30, 2008).

University of Alaska. Student Enrollment Services: FERPA Family Educational Rights and Privacy Act. http://www.alaska.edu/studentservices/ferpa/. (October 31, 2008).

University of Alaska. Important Notice: Comprehensive Notice of Privacy Policy and Procedures. http://www.alaska.edu/hr/benefits/open_enrollment/hipaa_privacy.pdf (July 7, 2008).

University of Alaska. Board of Regents' Policy, Part IV - Human Resources Chapter II: General Personnel Policies. http://www.alaska.edu/bor/policy/4p/p04-02.html (July 14, 2008).

University of Alaska Anchorage. Chapter VI: Human Research Subjects Policy and Procedure. http://www.uaa.alaska.edu/facultyservices/upload/HANDBOOK%20Chapter%20VI.dot (July 9, 2008).

University of Alaska Anchorage. Office of the Registrar: Access to Student Records University Student Educational Records (FERPA) Policy. http://www.uaa.alaska.edu/records/app/ferpa.cfm. (May 25, 2008).

University of Alaska Fairbanks. Center for Health and Counseling: Notice of Privacy Practices. http://www.uaf.edu/chc/privacy.html (July 11, 2008).

University of Alaska Fairbanks. Office of Research Integrity: Export Management General Guidance. http://www.uaf.edu/ori/Export_Management.htm (July 8, 2008).

University of Alaska Fairbanks. Research/Academic Policy: Safeguarding Confidential Information. http://www.uaf.edu/ori/Policies/Confidential_Information.pdf (July 8, 2008).

United States Department of Education. Family Educational Rights and Privacy Act (FERPA): http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html (May 28, 2008).

VISA, Card Holder Security Program. http://usa.visa.com/merchants/risk_management/cisp_overview.html (September 3, 2008).