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.

D xda R

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

dai-113(nf)-1(s)-20eee-31(r)11(m)m31(ent)-1(ss)]TJ 0f8(o)om(A)44ppaa sa o

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 nats Exam 22(3 -6.022 .3(d)]TJ 37</MCI.03335(s)-l)-53 Tw 14.804 0 1 [(A)-51(at)87(a)-34(t)-20TT(sd-13(a)(a)20 -0

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 [illegible] is classified, data custodians should use cauti-7(s)-33(e)-36( )]TJ 0 T

" ,QIRUPDWLRQ ι
protected by contract
" +XPDQ VXEMHFWV
identifiable research data
" 7UDGH VHFUHWV LQWHOOHFWXDO
property and/or proprietary
research
" $WWRUQH\ FOLHQW SULYLOHJHG
records
" 3D\PHQW &DUG ,QGXVWU\
(PCI)
" 8QLYHUVLW\ EDQNLQJ
records
" 5HVWULFWHG SROLFH UHFRUGV
(e.g., victim information,

Appendix A. Glossary

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 I2 Tc27(ntTd (yt1d)-c)-11<19.6 [(c)9 6(c)9 6a[19.T]TJ 0.022 Tw 0 -1.1-21(i)27(d of)-15(t)-27(hi)-27(

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

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

(8.4131lv United States Department of EdufEd6f >>BDC 8 of> Q!‰5ñ5'ZÑ0Ù5 4ÚÌ - 9ä 8P 5ó3& ŸY7p " "• †t Á