Data Classification Standard

Date Established: 5/24/2010
Date Last Revised: 5/24/2010
Date Posted to Library: 2/9/2011

Category: IT Policy
Responsible Office: CIO Office

Summary

All university data must be classified into one of the four categories described in this standard and protected using appropriate security measures consistent with the minimum standards for the classification level as described in related information/data security policies.

The Standard

This standard serves as a supplement to the Data Access and Security Policy. Adherence to the standard will facilitate applying the appropriate security controls to university data.

The objective of this standard is to assist data owners, data access managers, and data custodians in determining the level of security required to protect data on the systems for which they are responsible. The standard divides data into four categories:

Data Classification	Institutional Risk from Disclosure	Description	Examples
Category I: Regulated Private Data	High	Regulated data whose unauthorized access or loss could seriously or adversely affect UB, a partner, or the public. Security breaches of these data are subject to the NY State Information Security and Breach Notification Act and other federal, state, and industry rules and regulations.	• Social Security Number • Driver's License Number • State-issued Non-drivers ID Number • Bank/Financial Account Number • Credit/Debit Card Number • Electronic Protected Health Information • Passport Number • Central UB IT Authentication Credentials • Documents protected by Attorney Client privilege

Category II: Protected Data	Medium	Regulated data subject to FERPA or other federal, state, or business regulation; any data specifically exempt from release/disclosure to the public by state or federal statue. This includes data exempt from disclosure in NY State's Freedom of Information Law (FOIL). FOIL exempts data that if disclosed would constitute an unwarranted invasion of personal privacy.	• FERPA-protected data • Gramm Leach Bliley data and other data protected by law or regulation • Final Course Grades, Exam Questions or Answers • HR Employment Data • Law Enforcement Investigation Data, Judicial Proceedings Data o Includes Student Disciplinary or Judicial Action Information • Public Safety Information • IT Infrastructure Data • Collective Bargaining Negotiation Data, Contract Negotiation Data • Trade Secret Data • Protected Data Related to Research • University Intellectual Property • University Proprietary Data • Data protected by external non-disclosure agreements external • Inter- or Intra-Agency Data which are **not**: Statistical or factual tabulations; Instructions to staff that affect the public; Final agency policy or determination; External audit data
Category III: Internal Use Data	Low to Medium	All other non-public data not included in Category I or II	• University Financial Data • University Person Number • Meeting Minutes • Administrative process data • Data about decisions that affect the public • Licensed Software • Other University Non-Public Data*
Category IV: Public Data	None	All public data	• General access data, such as that on unauthenticated portions of **www.buffalo.edu**

This standard exists in addition to all other university policies and federal and state regulations governing the protection of the university's data. Compliance with this classification standard will not ensure that data will be properly secured. Instead, this standard should be integrated into a comprehensive information security plan.

All university data stored on university resources or other resources where university business occurs must be classified into one of the four categories. Based on the data classification, data owners,

trustees, custodians, and users are required to implement appropriate technical security measures to protect the data consistent with the university Minimum Security Standards for protecting the data. Category-I data has more stringent requirements than Categories II, III, and IV. All systems require some protective measures.

Note: Data that is personal to the operator of a system and stored on a university IT resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.

APPLICABILITY and SCOPE

This policy applies to all members of the University at Buffalo community, as well as to external vendors and contractors.

DEFINITIONS

Category I: Regulated Private Data – *Regulated private data* is defined using the definition of *private information* in the New York State Security and Breach Notification Act of 2005 as a foundation: bank account/credit card/debit card numbers, Social Security Numbers, state-issued drivers' license numbers, and state-issued non-drivers' identification numbers. To this list UB policy adds protected health information (PHI), computer passwords and other computer access protection data, and passport numbers. Note that Category I data are exempt from disclosure/release under the NY State Freedom of Information Law (FOIL). The Breach Notification Act requires that the University must disclose any breach of the data to NY residents. (State entities must also notify non-residents, see Information Security Policy P03-002 V3.3 *Part 12*) **-** pdf **.)**

Category II Protected Data – Includes University data not identified as Category-I data, but data protected by state and federal regulations. This includes FERPA-protected student records and electronic records that are specifically exempted from disclosure by the NY State Freedom of Information Law (FOIL). http://www.dos.state.ny.us/coog/foil2.html Such data must be appropriately protected to ensure that they are not disclosed in a FOIL request. FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy. Specific details on FOIL-excluded data are provided in the Appendix.

Category III Internal Use Data - Includes University non-public data not included in Category I (regulated private data) or Category II (protected data); Internal Use data includes Person Number, licensed software, as well as University business records, intellectual property, and any non-public data that is releasable in accordance with FOIL.

Category IV Public Data - General access data, such as that available on unauthenticated portions of www.buffalo.edu; Category IV data have no requirement for confidentiality.

CONTACT INFORMATION

For more information about this standard, contact the

Office of the CIO
517 Capen Hall
University at Buffalo
716-645-7979

RELATED POLICIES

Regulated Private Data Policy
Regulated Private Data Standards
Data Access and Security Policy

APPENDIX

RECORDS EXEMPTED FROM PUBLIC ACCESS (FOIL) – Taken from the NY State Department of Education, Office of the Chancellor Regulation[1]

A. The public has access to all records, except that the Department Of Education may deny access to records or portions of records that:

1. Are specifically exempted from disclosure by state or federal statute[2] (POL § 87(2) (a));
2. If disclosed, would constitute an unwarranted invasion of personal privacy (POL § 87(2) (b)) (see Section III below);
3. If disclosed, would impair present or imminent contract awards or collective bargaining negotiations (POL § 87(2) (c));
4. Are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which, if disclosed, would cause substantial injury to the competitive position of the subject enterprise (POL § 87(2) (d));
5. Are compiled for law enforcement purposes and which, if disclosed, would:
    a. interfere with law enforcement investigations or judicial proceedings;
    b. deprive a person of a right to a fair trial or impartial adjudication;
    c. identify a confidential source or disclose confidential information relating to a criminal investigation; or
    d. reveal criminal investigative techniques or procedures, except routine techniques and procedures (POL § 87(2) (e)).
6. If disclosed, would endanger the life or safety of any person (POL § 87(2) (f));
7. Are inter-agency or intra-agency materials unless they are:
    a. statistical or factual tabulations or data;

[1] Complete regulation from the NY State Department of Education, Office of the Chancellor is available at: http://docs.nycenet.edu/docushare/dsweb/Get/Document-84/D-110__1-9-03.pdf

[2] For example, FERPA, the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g.

b. instructions to staff that affect the public;
c. final agency policy or determinations; or
d. external audits, including but not limited to audits performed by the comptroller and the federal government (POL § 87(2) (g)).

8. Are examination questions or answers which are requested prior to the final administration of such questions (POL § 87(2) (h)); or

9. If disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures (POL § 87(2) (i)).

B. The release of and access to student records is governed by FERPA (the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g). See Chancellor's Regulation A-820, *Student Records: Confidentiality, Access, Disclosure and Retention.* Generally, information that would tend to identify a student, including but not limited to his/her name, student identification number and parent's name, must be redacted from documents prior to their release. However, if the requester represents the parent or eligible student whose record he/she is requesting and provides a written consent or release, the personally identifying information for his/her client will not be redacted (see Attachment No. 1).