Data Classification Standard

Date Established: July, 2011
Date Last Revised: January, 2016
Date Published: February, 2012
Category: IT Policy
Responsible Office: CIO Office

Summary

In support of the University’s Asset Classification Protocol, a campus protocol published under the Asset Classification Security Domain, all University data must be classified into one of the three 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 security standards, procedures, and guidelines.

The Standard

This standard serves as a supplement to the Asset Classification Protocol. Adherence to the standard will facilitate applying the appropriate security controls to University data.

The objective of this standard is to assist Data Owners, their designees, and Data Custodians¹ in determining the level of security required to protect data for which they are responsible. The standard divides data into three categories:

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Risk from Disclosure</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Category I: Protected Data: Personally Identifiable or Regulated | High-Medium | Personally Identifiable data includes information whose unauthorized access or loss could seriously or adversely affect UAlbany; an authorized, contracted partner; specific individuals, or the public. Security breaches of this information are subject to the NY State Information Security and Breach Notification Act and other federal, state, and industry rules and regulations. Regulated data includes information subject to FERPA or other federal, state, or business regulations (e.g., HIPAA, Red Flag Rules) that require specific levels of protection to prevent its unauthorized modification or use. | Statutory Data
  - 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-HIPAA
  - FERPA-protected data
  - Gramm Leach Bliley data and other data protected by law or regulation
  - Passport Number
  - DOD contracted “Applied Research”
  - Electronic Credentials (PINs, Passwords, Tokens, etc.)

Declared Data
  - System Administrator/PeopleSoft IAS Authentication Credentials
  - Documents protected by Attorney Client Privilege

¹ Data Owners are the business, academic, or research entities that are primarily responsible for collecting, creating, or using the data. Data Custodians are responsible for implementing the Data Owners decisions regarding access and usage.
<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Risk from Disclosure</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Category II:** Internal Use Data | Medium-Low | Category II includes non-public, internal use information that is not subject to state or federally mandated protections. This includes data exempt from disclosure in NY State’s Freedom of Information Law (FOIL), as well as information that would normally require a FOIL request for public release. | • Other 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/Contract Negotiation Data
• Trade Secret Data
• Protected Data Related to Research
• University Intellectual Property
• University Proprietary Data
• Data protected by non-disclosure agreements
• University Financial Data
• Albany/Empl_ID
• Meeting Minutes
• Administrative process data
• Data about decisions that affect the public
• Licensed Software
• 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 (See Appendix) |
| **Category III:** Public Data | None | All public data | • General access data, such as that on unauthenticated portions of www.albany.edu |

**DATA CLASSIFICATION and SECURITY CONTROLS REQUIREMENTS**
All University data stored on University systems, or non-University owned resources where University business is transacted, must be classified into one of the three categories. Based on the data classification, Data Owners, Trustees, Data Custodians, and users are required to implement appropriate administrative, technical, and physical controls to protect the data [see the accompanying Minimum Security Controls document]. Category-I data has more stringent requirements than Categories II and III. All systems require some protective measures.

When information from multiple classifications is co-located on the same system without effective means of isolation, or within the same repository, database, archive, or record, the Minimum Security Controls of the category representing the highest institutional risk must be applied. As an example, if names and social security numbers were included in meeting minutes, then Category I protections would be required for that document.
These requirements exist in addition to all other university policies and federal and state regulations governing the protection of University data. Compliance with this requirement alone will not ensure that data will be properly secured. Rather, data classification should be considered an integral part of a comprehensive information security plan.

Note: Consistent with the notion of Incidental Use, personal data belonging to employees stored on a University IT resource is not considered University data.

**APPLICABILITY and SCOPE**
This protocol applies to all members of the University at Albany community, as well as to external vendors and contractors who receive and maintain collections of University data.

**DEFINITIONS**

**Category I: Protected Data: Personally Identifiable or Regulated**
*Regulated private data* includes: information defined as *private information* (i.e., personally identifiable information) in the *New York State Information Security Breach and Notification Act of 2005*: i.e., bank account/credit card/debit card numbers, Social Security Numbers, state-issued drivers’ license numbers, and state-issued non-drivers’ identification numbers. Additionally, the University at Albany declares protected health information (PHI), administrative authentication credentials, and passport numbers as Category 1 data.

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 - [http://its.ny.gov/document/information-security-policy](http://its.ny.gov/document/information-security-policy).)

*Regulated protected data* includes data protected by state and federal regulations. This includes FERPA-protected educational records, protected health information (HIPAA), and other records governed by state and federal laws and regulations.

Note that Category I data is exempt from disclosure/release under the NY State Freedom of Information Law (FOIL) ([http://www.dos.ny.gov/coog/foil2.html](http://www.dos.ny.gov/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 II: Internal Use Data** - Includes University non-public data not included in Category I (Personally Identifiable or Regulated). Internal Use data includes the Albany ID/Empl_ID, licensed software, as well as University business records, intellectual property, certain types of information that would constitute an unwarranted invasion of personal privacy, and any non-public data that would generally require a FOIL request prior to release.

**Category III: Public Data** - General access data, such as that available on unauthenticated portions of [www.albany.edu](http://www.albany.edu); Category III data has no special requirements for confidentiality.
CONTACT INFORMATION

Office of the CIO
University at Albany
ITB 102
518-956-8080

RELATED PROTOCOLS

Protection and Use of Faculty, Staff, and Student Identifiers
Media Disposal, Destruction, and Redeployment

APPENDIX

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

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 (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;
   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.


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