Data Classification Standard

Date Established: July, 2011
Date Last Revised: July, 2018
Category: IT Policy
Responsible Office: ITS

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 Trustees, Stewards, and Custodians in properly classifying data to determine what controls are needed to protect its confidentiality, integrity, and availability. 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 1: Protected Data: Personally Identifiable or Regulated** | High-Medium | Personally Identifiable data includes information whose loss or unauthorized access could 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., GDPR, HIPAA, Red Flag Rules) that require specific levels of protection to prevent its unauthorized modification or exposure. | **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
- DOD contracted “Applied Research”
- Electronic Credentials (PINs, Passwords, Tokens, etc.)
- Federal Controlled but Unclassified Information (CUI)

**Declared Data**
- System Administrator/ PeopleSoft IAS Authentication Credentials
- Passport Number
- Documents protected by Attorney Client Privilege |
| **Category 2: Internal Use Data** | Medium-Low | Category 2 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  
  • 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 is not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination; external audit data (See Appendix) |
| **Category 3: 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. In general, data will self-classify based on its source or nature. Data Trustees, Stewards, Custodians, and users are required to implement and observe appropriate administrative, technical, and physical controls to protect the data [see the Category 1 Security Controls document]. Category 1 data has more stringent requirements than Categories 2 and 3. At minimum, all data requires some protective measures to guard against tampering.

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 1 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. 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 1: 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: 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 declares certain information such as administrative authentication credentials Category 1 data.

The Breach Notification Act requires that the University must disclose any breach of the data to NY residents. (State entities also must 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, federal, and business regulations. This includes FERPA-protected educational records, protected health information (HIPAA), and other regulated information such as that defined in the Payment Card Industry Data Security Standards (PCI-DSS), the Gramm Leach Bliley Act, the FTC’s Red Flag Rules, the EU’s General Data Protection Regulation (GDPR), federal Controlled but Unclassified Information (CUI), etc.

Note that Category 1 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 it is 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 2: Internal Use Data - Includes University non-public data not included in Category 1 (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 3: Public Data - General access data, such as that available on unauthenticated portions of www.albany.edu; Category 3 data has no special requirements for protecting confidentiality.