Data Classification Policy

**Functional Area:** Information Technology Services (IT Services)

**Applies To:** All users of Armstrong’s network services

**Policy Reference(s):**
- Responsible Access and Use of Information Technology Resources and Services
- Board of Regents’ Business Procedures Manual, Section 12
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- USG IT Handbook

**Date Issued:** January 20, 2014

**Date of last review:** January 20, 2014

**Date of next review:** July 1, 2014

**Page(s):** 3

---

**Responsible Person**

This policy will be re-evaluated on or about the first day of July each calendar year to determine whether all aspects of the policy are up to date and applicable in the current business environments, and will be revised as necessary. The Information Security Officer is responsible for review and accuracy of this policy.

---

**Purpose / Rationale**

The purpose of the policy is to define the data classifications for University data and the responsibilities for the protection of such data. While performing job duties at Armstrong Atlantic State University, all employees will require access to many types of information or data, some of which may be considered sensitive (e.g., budget information) or confidential (e.g., social security numbers). It is important that faculty, staff, student workers, and any contracted entity working on behalf of Armstrong Atlantic State University with access to data understand their responsibilities for identifying, transmitting, re-distributing, storing, or disposing of these categories of information.

---

**Definitions**

Data Owner: University employee who can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness
To handle data properly, it is important that employees know the various data types and what laws or standards, if any, might govern their use. For example, student education records are governed by FERPA, personal health information is governed by HIPAA, and credit card information is governed by PCI-DSS. In contrast, directory information can be made available to the general public. In order to implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, Armstrong Atlantic State University classifies its data and use into three (3) levels:

- Level 1: Public Data
- Level 2: Sensitive Data
- Level 3: Confidential Data

Regardless of the category, data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures should be implemented commensurate with data value, sensitivity, and risk.

Sensitive data and confidential data will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, and/or violate laws, policies or University contracts.

Level 1: Public Data:

Public data is explicitly approved for distribution to the public. This information may be freely disseminated without a significant risk of harm to the University or its affiliates.

Examples: Advertising, course information, directory information, job postings, and press releases.

Level 2: Sensitive Data:

Sensitive data elements include those which Armstrong protects to mitigate institutional risk. Sensitive data requires users to obtain specific authorization for access. Good faith acquisition or distribution of sensitive data by or between University employees and/or contracted entities for a legitimate purpose is allowed, provided that the information is not used in violation of applicable laws or policies or in a manner that harms or poses a reasonable threat to the security, confidentiality or integrity of the personal information. When a risk of identity theft or other fraud is not reasonably likely to occur with an unauthorized disclosure of this information, notification of affected individuals will not be required.

Examples: Budget information, research that has not been completed or published, and general contracts.

Note: Per Board of Regents Business Procedures Manual, it is assumed that all administrative output from the central administrative systems, such as Banner and PeopleSoft, are classified as sensitive unless otherwise indicated.
Level 3: Confidential Data:

Confidential data includes information that if improperly used or disclosed could adversely affect the ability of the University to accomplish its mission, as well as information protected by laws and/or policies to include records about individuals requesting protection under FERPA, or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Unauthorized disclosure of information at this level will often require notification of affected individuals in accordance with applicable statutes.

Personally Identifiable Information (PII) is covered under confidential data classification.

Examples: Social Security Numbers, personnel records, credit card numbers, medical records, student data that is not considered directory information, University system log-in credentials, information protected by non-disclosure agreements, and confidential research.

Nothing in this policy should be construed to supplant the special jurisdictions and procedures set forth by federal or state laws or USG policies.