**AIMS COMMUNITY COLLEGE**

**ACCEPTABLE USE OF INFORMATION TECHNOLOGY**

**DATA CLASSIFICATION STANDARD**

**Purpose**

The purpose of this standard is to provide the College community with a framework for safeguarding information from risks including, but not limited to, unauthorized use, access, disclosure, modification, loss, or deletion.

**Scope**

This standard applies to all faculty, staff or third-party vendors of Aims Community College with access to store, process or transmit College business data.

1. **Data Classification**

Data classification is the process of organizing data into predetermined classification levels so that it may be used and protected more effectively. The classification level applied to the data is based on its level of sensitivity and the impact to the College should it be disclosed, altered or destroyed without authorization. Properly classified data is easier to locate, maintain and secure. All institutional data should be classified into one of three sensitivity levels or classifications: Confidential, Internal or Public.

|  |  |
| --- | --- |
| **Confidential** | |
| **Description** | **Examples** |
| * Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the College or individual. * Data protected by state or federal privacy regulations and data protected by confidentiality agreements. * Confidential data must not be disclosed to parties without explicit authorization from the Data Steward. * Physical Confidential data must be stored in a locked drawer or room or an area where access is controlled by a guard, cipher lock, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know. * The highest level of security controls should be applied to Confidential data. | * Personally Identifiable Information (PII) * FERPA-protected data (non-directory information) * Student or employee ID number in combination with a first name or first initial and last name * Payment card data subject to PCI DSS * Data protected by the Gramm–Leach–Bliley Act (GLBA) * Social security number * Date of Birth * Driver's License/State ID Number * Bank/Financial Account Number * Credit/Debit Card Number * Visa/Passport Number * Donor contact information and non-public gift information * Passwords and PINs * Non-disclosure agreements (NDA) |
|  | |
| **Internal** | |
| **Description** | **Examples** |
| * Data should be classified as Internal when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the College or individual. * Physical Internal data must be stored in a closed container (e.g., file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use. | * Student and employee data not containing Confidential elements * Non-public policies, manuals, and contracts * Internal memos and email, non-public reports, budgets, and plans * Financial transactions not including Confidential data * Engineering, design, and operational information regarding infrastructure |
|  | |
| **Public** | |
| **Description** | **Examples** |
| * Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College or individual. * While little or no controls are required to safeguard Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. | * Faculty/Staff directory data * FERPA directory data * Campus maps * Public-facing websites * Policy and procedure manuals designated by the owner as public * Job postings * Information in the public domain |

1. **Standard Details**
2. **Classification**
3. All institutional data should receive a classification level. Data missing an express classification shall be treated as Internal until otherwise classified.
4. While data classification is a shared responsibility, the Data Steward (commonly referred to as “Data Custodian” at Aims) is ultimately accountable for the proper classification of the data for which they are responsible. The Data Steward oversees the lifecycle of the data and is best qualified to make classification decisions because he or she has the most knowledge about the use of the data and its value to the College. The Data Steward is also responsible for determining who has access to the data.
5. In some instances, it may be appropriate to apply a single classification to a collection of data that is similar in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Confidential even though the student's name and address may be considered Public information.
6. **Data Lifecycle**
   1. The collection, use, and retention of data, especially sensitive data, should be limited to the least amount necessary to conduct a business goal. Doing so limits the potential negative consequences of a data breach involving such data and the costs and efforts associated with maintaining the data.
   2. Maintaining data is a continuous ongoing process all users of data are engaged in. Because of this, data should be reviewed regularly to determine whether it is still relevant and necessary for meeting Aims purpose and mission. Data that is no longer needed to conduct a business goal should be deleted. For more information on document retention, see the Aims Document Retention Schedule 3-500A: <https://www.aims.edu/policies/manual/section3/3-500A.pdf>
7. **Data Storage and Distribution**

Acceptable means of storing and/or distributing College data in digital format are determined according to the classification level of the data. While not an exhaustive list, the following resources may be used for their respective classification levels:

**Confidential**

* Banner (as appropriate)
* Banner Document Management (BDM)
* Box (limited licenses)
* College-owned laptops that have full disk encryption implemented. Confidential data should be removed from laptops as soon as it is no longer required. (Contact IT to determine if your computer has full disk encryption or to get full disk encryption.)

**Internal**

* Any methods used for Confidential Data.
* The “G:” or “Z:” drives which are network drives on a shared server
* College-owned web services which require an Aims network authorization to access the content.
* Google Apps (Gmail, Drive, Calendar, Hangouts, etc.)
* Smartsheet
* Third-party writing assistant software (e.g., Ginger, Grammarly, Reverso, etc.)

**Public**

* Any methods used for Confidential Data and Internal Data.
* Local hard drives on your personally owned workstations or laptops
* College or personal websites accessible to the public

1. **Incident Reporting**Report the misuse or compromise of systems that handle, store, or propagate protected data immediately to [it.security@aims.edu](mailto:it.security@aims.edu).
2. **Reference**
3. **Personally Identifiable Information**

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Examples of PII include, but are not limited to a first name or first initial and last name in combination with any one or more of the following data elements that relate to an individual:

* Social security number
* Student, employee, military, or passport identification number
* Other indirect identifiers such as a date of birth
* Driver's license number or identification card number
* Medical information
* Health insurance identification number
* Biometric data
* Photos, videos, and voice recordings

The following are also considered PII:

* A username or email address, in combination with a password or security questions and answers, that would permit access to an online account
* An account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account

1. **Payment Card Information**  
   Payment card information is defined the full Primary Account Number (PAN) or the full PAN along with any of the following elements:
2. Cardholder name
3. Expiration date
4. Service code
5. Contents of a credit card’s magnetic stripe
6. CAV2, CVC2, CVV2 or CID values
7. PIN or PIN block

1. **Personally Identifiable Education Records**  
   Personally Identifiable Education Records are described in the [Family Educational Rights and Privacy Ac](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)t (FERPA) of 1974 (20 USC §1232g) and are defined as any Education Records that contain one or more of the following personal identifiers:
2. Name of the student
3. Name of the student’s parent(s) or another family member
4. Social security number
5. Student number
6. A list of personal characteristics that would make the student’s identity easily traceable
7. Any other information or identifier that would make the student’s identity easily traceable
8. **Related Regulations**

This standard is a component of Aims Community College information security program that is intended to comply with:

1. Payment Card Industry Data Security Procedure (PCI-DSS)
2. Family Educational Rights and Privacy Act of 1974 (FERPA)
3. Gramm–Leach–Bliley Act (GLBA)
4. Federal, state and local law
5. Other regulations as appropriate
6. **Exceptions**

Only the Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this standard. Any requests for exceptions shall be made using the “Request for Procedure Exception” form and a copy maintained by the CIO.

1. **Violations**

Any user found to have violated this standard may be subject to disciplinary action, up to and including termination and notification of the appropriate law enforcement authorities of any unlawful activity.

1. **Definitions**
2. **Family Education Rights and Privacy Act (FERPA):** FERPA deals with student “education records,” defined to mean (with a few exceptions) records containing information directly related to a student that are maintained by a school or its agent.
3. **Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information (GLBA):** The Gramm Leach Bliley Act (GLBA) requires that financial institutions safeguard nonpublic customer data, limit disclosures of such data, and notify customers of their information sharing practices and privacy policies.
4. **Third Party Vendor**: Non-employee of Aims Community College who is contractually bound to provide services to College.
5. **Users:** Any Aims Community College Faculty, Staff, Students or partner with access to the College systems, or electronic information resource.