SNOW COLLEGE

Policy #12.2
Date Approved: 12-18-2003
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: DATA CLASSIFICATION AND HANDLING POLICY

1.0 PURPOSE

The purpose of this policy is to establish a framework for classifying and handling college data based on its level of sensitivity, value and criticality to the college as required by the College's information security plan. Classification of data will determine the baseline security controls for the protection of data. This policy applies to all College employees who access, process, or store sensitive College data.

2.0 DEFINITIONS

2.1. *Personally Identifiable Information (PII)*. Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are Credit Card and Social Security numbers.

2.2. *Data Owner*. An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the College.

2.3. *Data Custodian*. Employee of the college who has administrative and/or operational responsibility over information assets.

2.4. *Institutional Data*. All data owned or licensed by the College.

2.5. *Information Assets*. Definable pieces of information in any form, recorded or stored on any media that is recognized as “valuable” to the college

2.6. *Non-public Information*. Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

3.0 POLICY

3.1. Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the College should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels (tiers), or classifications:

3.1.1. **Personally Identifiable Information (PII).** Data is classified as PII when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the College or its affiliates. Examples of PII data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied. Access to PII data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the college who require such access in order to perform their job "need-to-know". Access to PII data must be individually requested and then authorized by the Data Custodian who is responsible for the data. PII data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of PII data include official student grades and financial aid data, social security and credit card numbers, and individuals' health information.

3.1.2. **Internal Data**. Data is 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 its affiliates. By default, all information assets that are not explicitly classified as PII or public data should be treated as internal data. A reasonable level of security controls should be applied to internal data.

Access to Internal data must be requested from, and authorized by, the data owner who is responsible for the data. Access to internal data may be authorized to groups of persons by their job classification or responsibilities "role-based" access, and may also be limited by one's department.

Internal data is moderately sensitive in nature. Often, internal data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the College should this information not be available when needed is typically moderate. Examples of internal data include official College records such as financial reports, human resources information, some research data, and budget information.

3.1.3. **Public Data.** Data is classified as public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data. Public data is not considered sensitive;

therefore, it may be granted to any requester or published with no restrictions. The integrity of public data should be protected. The appropriate data owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should public data not be available is typically low (inconvenient but not debilitating). Examples of public data include directory information, course information and research publications.

3.2. Determining Classification

3.2.1. The goal of information security, as stated in the College's Information Security Policy, is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the College if confidentiality, integrity or availability of the data is compromised.

3.3. Data Handling Requirements

3.3.1. For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

3.3.2. The attached table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

3.3.3. Predefined Types of PII Information Assets. Based upon state, federal, and contractual requirements that Snow College is bound by, the following information assets have been predefined as PII data and must be protected.

3.3.3.1. Personally Identifiable Education Records. Covered under FERPA.

Personally Identifiable Education Records are defined as any education records that contain one or more of the following personal identifiers:

- Student Badger ID Number
- Grades, GPA, Credits Enrolled
- Social Security Number
- A list of personal characteristics or any other information that would make the student's identity easily traceable

3.3.3.2. Personally Identifiable Financial Information(PIFI). Covered under GLBA. For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- Date of Birth
- Financial account number in combination with a security code, access code or password that would permit access to the account

3.3.3.3. Payment Card Information. Covered under PCI DSS. Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe
- Contents of Card Chip

3.3.3.4. Protected Health Information (PHI). Covered under HIPAA. PHI is defined as any individually identifiable information that is stored by a covered entity, and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual
- PHI is considered individually identifiable if it contains one or more of the following identifiers:
  - Name
  - Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
  - All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89

- Telephone/Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

- If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered individually identifiable and; as a result, would not be considered PHI.

4.0 REFERENCES

12.4 Information Security Policy

12.5 Information Technology Acceptable Use Policy

Information Security Classification Standard

Classification	Definition	Access Restrictions	Transmission	Storage	Disposal
Public	Information deemed to be public by legislation or policy. Information is in the public domain. Examples include annual reports, public announcements, the telephone directory, and specific categories of employee and student information.	No restrictions on access.	No special handling required.	No special safeguards required.	Media can be recycled.
Internal Use	Information not approved for general circulation outside the College. Loss would inconvenience the College or management; disclosure is unlikely to result in financial loss or serious damage to credibility. Examples include internal memos, minutes of meetings, internal project reports.	Access limited to employees and other authorized users.	No special handling required.	Access controlled by physical (locks) or electronic (passwords) safeguards.	Shredded or erased media.
Personally Identifiable Information (PII)	Information that is available only to authorized persons. Loss could seriously impede the College's operations; disclosure could have a significant financial impact or cause damage to the College's reputation. Examples include specific categories of employee and student information, unit budgets, accounting information, and information protected by legal privilege.	Access limited to those with a demonstrated need to know and official approval.	Encryption mandatory for public networks. Encryption optional for internal networks.	Access controlled by physical (locks) or electronic (passwords or two-factor authentication) safeguards	Shredded, degaussed or destroyed.