

### I. PURPOSE AND SCOPE

This rule describes requirements for managing college electronic data and information assets and supports the [Data Classification Guidelines](#) of the college's Data Governance Committee.

### II. DEFINITIONS

- A. **Electronic Resource:** any resource used for electronic communication, including but not limited to internet, e-mail, and social media.
- B. **Information Asset:** data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling college to perform its business functions.
- C. **Information System:** an application or group of servers used for electronic storing, processing, or transmitting any college data or information asset.
- D. **IT Resource:** any computer resource used to perform college business operations including, but not limited to, the creation, access, storage, processing, and transmission of information assets. (i.e., server, workstation, mobile device, networking device, web camera, etc.).
- E. **IT Technician:** a college employee who uses industry best practices to develop, administer, manage, and monitor computer resources and assets that support the college's IT infrastructure and ensure compliant IT system security.
- F. **Sensitive Data:** any data whose release could have a material adverse effect on the college's interest or on personal privacy rights. This data type is in the Data Classification and Encryption Rule.

### III. PROCEDURES

- A. Data Classification Guidelines
  - 1. College electronic data must be classified and continually evaluated to determine the appropriate classification according to the Data Classification Guidelines. These data classification guidelines in no way supersede any state or federal government classifications.
  - 2. These data classifications apply to all electronic data that the college owns or has custody of, wherever it may be stored, including:
    - a. data stored at data center;
    - b. data accessed by or stored remotely on IT resources; and
    - c. college data that is stored with contracted third parties including Business Associates, cloud service providers, vendors, contractors, and temporary staff.

3. When a specific set of data is classified as fitting within a combination of two or more of the data classifications, that data shall be managed according to the most restrictive/secure applicable data classification.

#### B. Data Encryption

1. All data encryption decisions must be formally documented and shall be considered in the context of the data at rest and data in motion.
2. IT technicians must work in cooperation with the Information Security Office (ISO) to determine encryption requirements, as these requirements may change due to the college's technology equipment, an emerging threat, and/or in response to regulatory requirements.

#### C. Data At Rest Requirements

1. College data stored outside the college:
  - a. Critical data: encryption is required in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.
  - b. Restricted data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.
  - c. College Internal and Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.
2. College data stored within the college:
  - a. Critical data on all mobile devices and laptops must be encrypted in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.
  - b. Critical data on Servers and Information Systems will be encrypted as directed by risk analysis in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.
  - c. Restricted data: encryption is strongly recommended and should be in accordance with the data steward requirements.
  - d. College Internal and Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.

#### D. Data In Motion Requirements

1. College data transmitted outside of the college's network:
  - a. Critical data: encryption is required in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance
  - b. Restricted data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.
  - c. College Internal and Public Data: encryption is optional and should be in

accordance with the Data Steward's requirements.

2. College data transmitted within the college network

- a. Critical data: encryption is recommended in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.
- b. Restricted data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.
- c. College Internal and Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.

E. Data Classification

1. Data Stewards, or their designee, in consultation with the Data Governance Council and CIO/CISO, shall classify College electronic data according to this rule, and data shall be continually evaluated to determine the appropriate classification. This rule shall be used to determine the appropriate data classification for data created, stored, processed, or transmitted using IT resources, information systems, and electronic resources across the College. Under this rule, data shall be classified in accordance with external regulatory, internal regulatory, and other contractual requirements. This rule does not supersede state or federal government classifications.
2. These data classifications apply to electronic data that the College owns or has custody of, wherever it is stored. This includes data stored at data centers, data accessed by or stored remotely on IT Resources, and College data that is stored with contracted third parties, including business associates, cloud service providers, vendors, contractors, and temporary staff.
3. Data that is classified as fitting in multiples classifications shall be managed according to the most restrictive/secure applicable data classification.

F. Data Classification Model

	<b>Restricted / Critical Data (High level of sensitivity)</b>	<b>Sensitive Data - College Internal (Moderate level of sensitivity)</b>	<b>Public Data (Low level of sensitivity)</b>
<b>Legal Requirements</b>	Protection of data is required by federal or state law or regulation, or contractual obligation, and may be subject to data breach notification requirements.	Protection of data is required by the Data Steward, and the appropriate confidentiality agreement, Access <a href="#">SLCC Data Roles</a> for more information about Data Stewards.	Outside of device Encryption (Section III.E), Protection of data is at the discretion of the Data Steward. Access <a href="#">SLCC Data Roles</a> for more information about Data Stewards.
<b>Access</b>	Only authorized individuals with approved access, a business need to know, and the appropriate confidentiality agreement.	Only authorized individuals with approved access, a business need to know, and the appropriate confidentiality agreement.	General public within the confines of the law.
<b>Data Types</b>	<ul style="list-style-type: none"> <li>• Personally identifiable Information (PII)</li> <li>• Protected Health Information (PHI)</li> <li>• Payment Card Industry (PCI)</li> <li>• Financial information</li> <li>• Donor information</li> <li>• Authentication information</li> </ul>	<ul style="list-style-type: none"> <li>• Intellectual Property</li> <li>• Designated non-public academic activity information (DNPAAI)</li> <li>• Employee information</li> <li>• Student information</li> <li>• Current litigation material</li> <li>• Contracts</li> <li>• Physical building and utilities detail documentation</li> </ul>	<ul style="list-style-type: none"> <li>• SLCC history</li> <li>• Business contact data</li> <li>• Company directory</li> <li>• Maps</li> </ul>

G. Restricted Data Types

1. Personally Identifiable Information (PII)

- a. PII is protected by federal and state laws and regulations, including federal regulations administered by the U.S. Department of Homeland Security (DHS), and is defined by DHS as information which allows the identity of an individual to be directly or indirectly inferred. If PII is lost, compromised, or disclosed without authorization, it could result in

substantial harm, embarrassment, inconvenience, or unfairness to an individual. PII will be released in accordance with the Utah Government Records Access Management Act (GRAMA) or other disclosures required by law. PII includes but is not limited to:

- i. any of the following stand-alone elements:
  - a) full Social Security number (SSN)
  - b) driver's license or state ID number
  - c) passport number
  - d) visa number
  - e) Alien Registration Number (A-Number)
  - f) fingerprints or other biometric identifiers
- ii. full name in combination with:
  - a) mother's maiden name
  - b) date of birth
  - c) last four digits of SSN
  - d) citizenship or immigration status
  - e) ethnic or religious affiliation

## 2. Protected Health Information (PHI)

- a. PHI is protected by the federal Health Insurance Portability and Accountability Act (HIPAA) and includes all individually identifiable information, in any medium, that relates to the individual's past, present, or future health, health care, or payment for the provision of healthcare that identifies the individual for which there is a reasonable basis to believe it can be used to identify the individual. Please contact the Privacy Office with questions regarding HIPAA, PHI, and deidentification. PHI specifically includes but is not limited to:

- i. any PII field in combination with the following identifiers:
  - a) diagnosis or ICD code
  - b) treatment or CPT code
  - c) provider name or number
  - d) physician name
  - e) treatment date
  - f) patient notes
  - g) psychiatric notes
  - h) patient photos
  - i) radiology images

## 3. Payment Card Industry (PCI) Data

- a. PCI data is subject to the Payment Card Industry Data Security Standards (PCI-DSS), developed by the PCI Security Standards Council and adhered to by the College. PCI data includes but is not limited to:

- i. Cardholder data:

- a) primary account number (PAN)
- b) cardholder name
- c) service code
- d) expiration date

ii. Sensitive Authentication Data (SAD):

- a) full track data (magnetic stripe data or equivalent on a chip)
- b) card verification code (e.g., CAV2, CVC2, CVV2, CID)
- c) PINs/PIN blocks.

4. Financial Information

- a. Financial information is governed by the Financial Accounting Standards Board (FASB). Financial information includes monetary facts about Salt Lake Community College and/or other parties who participate in financial transactions with the College that are used in billing, credit assessment, loan transactions, and other similar activities, that shall be protected prior to release in accordance with GRAMA or other disclosures required by law. Financial information includes but is not limited to:

- i. taxpayer identification number
- ii. credit ratings
- iii. account numbers
- iv. account balances.

5. Donor Information

- a. Donor information is the PII of the donor in conjunction with the financial asset information of the donations to the College. Donor information includes but is not limited to:

- i. donor's full name
- ii. donor contact information
- iii. financial assets, including
  - a) securities donated
  - b) real estate donations
  - c) planned giving arrangements

6. Authentication Information

- a. Authentication information comprises tools and methods for managing digital authentication credentials. Authentication information includes but is not limited to:

- i. passwords
- ii. certificates
- iii. cryptographic keys
- iv. multifactor authentication (MFA) codes
- v. tokens
- vi. API keys

## H. Sensitive Data Types

### 1. Intellectual Property

- a. Intellectual Property is electronic data that supports Inventions, as defined in College [Copyright Ownership and Intellectual Property - Policy 1.1.040](#).

### 2. Designated Non-Public Academic Activity Information (DNPAAI)

- a. Designated non-public academic activity information (DNPAAI) is information regarding academic activities of an individual member of the College community (including faculty, non-faculty academic personnel, staff, or students) that the individual has specifically designated as Sensitive Data. Such information may be reported to College administrators for purposes of evaluation of the individual's performance and shared with limited sets of other individuals for the purpose of furthering the academic activity. DNPAAI is considered as Sensitive Data, not intended to be made accessible to the general public. Types of information that an individual may choose to designate as DNPAAI, include, for example:
  - i. academic research or teaching activities involving use of live animal research subjects, or other controversial matters;
  - ii. academic research or teaching activities involving control of hazardous materials or technology which presents a high risk of harm to people or property; and
  - iii. academic service activities involving affiliation with an organization that, if made known to the general public, may result in risk of bodily or other harm to the individual.
- b. An individual who wishes to designate specific information as DNPAAI shall do so through the appropriate College procedures applicable for periodic reporting of academic activity information. For example, a faculty member submitting information to the College administration through the Faculty Activity Report (FAR) system designates whether each set of submitted information should or should not be made accessible to the general public as part of that person's Faculty Profile published by the College.
- c. Even for information which an individual has designated as DNPAAI, the College's ability and obligation to limit public access to that information is constrained by federal and state laws which allow certain types of information to be obtained on request, such as the Government Records Access and Management Act (GRAMA).

### 3. Employee Information

- a. Employee information is managed by Human Resources; is protected by state or federal laws and regulations, including regulations of the United

States Department of Labor; is associated with an employee or applicant for employment; and shall be protected prior to release in accordance with the Government Records Access Management Act (GRAMA).

Employee information includes but is not limited to the following:

- i. contents of Employment applications, other than Restricted Personally Identifiable Information (PII)
- ii. personnel files
- iii. performance evaluations
- iv. benefits information

#### 4. Student Information

a. Student information is protected by the federal Family Educational Rights and Privacy Act (FERPA), and includes records, files, documents, and other materials that contain information directly related to a student as a part of the student's education record or treatment record maintained by Salt Lake Community College or by a party acting for the Salt Lake Community College. Student information includes but is not limited to the following:

- i. grades
- ii. class lists
- iii. student course schedules
- iv. disciplinary records
- v. student financial records
- vi. payroll records for student employees (e.g., work study, assistantships, resident assistants)

#### 5. Current Litigation Material

a. Electronically stored current litigation material is information that pertains to a current litigation hold implemented by the College's Office of General Counsel, including but not limited to:

- i. Word, Excel, and PowerPoint documents
- ii. PDF documents
- iii. email and chat records
- iv. calendar items
- v. electronic voicemail
- vi. Removeable Media

#### 6. Contracts

a. Contracts are electronic copies of agreements to which the College is a party that may contain private information.

#### 7. Physical Building and Utilities Detail Documentation

- a. Physical building and utilities detail documentation is documentation of the details of physical buildings (including blueprints and images), utility connection points, and communication closet and fiber hub locations.

I. Information Security Program Documentation

1. The Chief Information Security Officer must maintain all information security program documentation and make it available for all college workforce members and Users.
2. The Chief Information Security Officer must ensure that any action, activity, or designation required by the information security program documentation is maintained in paper and/or electronic form. All such documentation must be maintained as specifically required.
3. Employees must not destroy any information security program documentation before consulting with the Chief Information Security Officer.