Rule R4-004C: Data Classification and Encryption

Revision 2. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose

The purpose of this Data Classification and Encryption Rule is to describe requirements for managing University electronic data and Information Assets.

B. Scope

The scope of this rule is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents.

This rule supports section C, titled Data Classification and Encryption, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this rule. In addition, the terms below apply for the limited purposes of this rule.

A. Cloud Service Provider – An IT company that provides services such IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (software as a service). The processing and storage resources provided are on-demand, scalable, and accessed via the internet. Examples of Cloud Service Providers are Amazon Web Services (AWS) and Google Cloud Platform (GCP).

B. Data Steward – The same as that term is defined in Policy 4-001.

C. HIPAA – Health Information Portability and Accountability Act

D. Inventions – The same as that term is defined in Policy 7-002.

E. PHI – Protected Health Information

F. PII – Personally Identifiable Information

G. Removable Media – Physical media that is attached to or easily removed from an electronic device (e.g., IT Resource, Information System, Workstation, Mobile Device) on which Information Assets are stored for backup and sharing purposes (e.g., USB drives, thumb drives, external hard drives, DVDs, CDs).

III. Rule

A. Data Classification

1. Data Stewards, or their designee, in consultation with the Chief Information Security Officer and UIT/ITS executive leadership, shall classify University 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 University. 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 University 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 University 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.

B. Data Classification Model

	Restricted Data (High level of sensitivity)	Sensitive Data (Moderate level of sensitivity)	Public Data (Low level of sensitivity)
Legal Requirements	Protection of data is required by federal or state law or regulation, or contractual obligation, and may be subject to	Protection of data is required by the Data Steward, and the appropriate confidentiality agreement,	Outside of device Encryption (Section III.E),

	data breach notification requirements.	Access Policy 4-001 for more information about Data Stewards.	protection of data is at the discretion of the Data Steward. Access Policy 4-001 for more information about Data Stewards.
Access	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.
Data Types	• Personally Identifiable Information (PII) • Protected Health Information (PHI) • Payment Card Industry (PCI) • Financial information • Donor information • Authentication information	• Intellectual Property • Designated non-public academic activity information (DNPAAI) • Employee information • Student information • Current litigation material • Contracts • Physical building and utilities detail documentation	• University of Utah history • Business contact data • Company directory • Maps

C. 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 shall be protected prior to release 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); or

            F. fingerprints or other biometric identifiers; and

        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; or

            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; or

        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 University. PCI data includes but is not limited to:

        i. Cardholder data:

            A. primary account number (PAN);

            B. cardholder name;

C. service code; and

D. expiration date; and

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); and

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 the University of Utah and/or other parties who participate in financial transactions with the University 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; and

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 University. Donor information includes but is not limited to:

i. donor’s full name;

ii. donor contact information; and

iii. financial assets, including:

A. securities donated;

B. real estate donations; and

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; and

vi. API keys.

D. Sensitive Data Types

1. Intellectual Property

a. Intellectual Property is electronic data that supports Inventions, as defined in University Policy 7-002.

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 University 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 University 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 University procedures applicable for periodic reporting of academic activity information. For example, a faculty member submitting information to the University 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 University.

c. Even for information which an individual has designated as DNPAAI, the University'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; and

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 the University of Utah or by a party acting for the University of Utah. 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; and

      vi. payroll records for student employees (e.g., work study, assistantships, resident assistants).

5. Current Litigation Material

a. Current litigation material is electronically stored information that pertains to a current litigation hold implemented by the University'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; and

vi. Removeable Media.

6. Contracts

a. Contracts are electronic copies of agreements to which the University is a party that create obligations enforceable by law.

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.

E. Data Encryption

1. Data at Rest Requirements

a. All devices storing, processing, creating, or transmitting University data, where technically feasible, shall be Encrypted.

2. Data in Motion Requirements

a. For University data transmitted outside of the University's network:

i. Encryption is required; and

ii. the Encryption method utilized must be consistent with any applicable guidelines from state or federal authorities.

b. For University data transmitted within the University's network:

i. Encryption is recommended; and

ii. the Encryption method utilized must be consistent with any applicable guidelines from state or federal authorities.

F. Cloud Service Provider Use

1. The University may not store Restricted Data with a Cloud Service Provider unless a contractual agreement that protects the confidentiality of the information and data is in place between the University and the cloud service provider.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources

A. Policies/ Rules.

1. Policy 4-004: University of Utah Information Security Policy

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources. [*reserved*]

V. References

A. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy

B. Family Educational Rights and Privacy Act of 1974 ("FERPA", 20 U.S.C. § 1232g)

C. Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)

D. ISO 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls

E. NIST 800 Series, Federal Information Security Standards

F. Policy 3-070: Payment Card Acceptance

G. Policy 4-001: University Institutional Data Management

H. Policy 4-003: World Wide Web Resources Policy

I. Policy 5-111: Disciplinary Actions and Dismissal of Staff Employees

J. Policy 6-400: Code of Student Rights and Responsibilities

K. Policy 6-316: Code of Faculty Rights and Responsibilities

L. Pub. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

M. Omnibus HIPAA Rule: 45 CFR Parts 160 and 164 - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

N. Utah Board of Higher Education Policy R345: Information Technology Resources Security

VI. Contacts

The designated contact officials for this Regulation are:

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History

A. Current version. Revision 2.
    1. Approved by President Randall as an Interim Rule on September 12, 2023 with effective date of September 12, 2023. Rule finalized with no changes after Board of Trustees approval of Policy 4-004 revisions on November 14, 2023.
    2. Legislative History
    3. Editorial Revisions
B. Previous versions.
    1. Revision 0. Effective date April 4, 2016.
C. Renumbering
    1. Not applicable.