Rule 4-004C Data Classification and Encryption Rev. 1

I. Purpose and Scope

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

B. 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: University of Utah Information Security Policy, apply for purposes of this Rule, including the following:

A. **Electronic Resource** – Any resource used for electronic communication, including but not limited to internet, Email, and social media.

B. **Information Asset** – Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling University to perform its business functions.

C. **Information System** – An Application or group of Servers used for the electronic storage, processing, or transmitting of any University data or Information Asset

D. **IT Technicians** – IT Technicians develop, administer, manage and monitor the IT Resources, Information Systems, and Electronic Resources that support the University's IT infrastructure, are responsible for the security of the IT Resources, Information Systems, and Electronic Resources they manage, and assure that security-related activities are well documented and completed in a consistent and auditable manner.

E. **IT Resource** – A Server, Workstation, Mobile Device, medical device, networking device, web camera or other monitoring device, or other device/resource that is a) owned by the University or used to conduct University business regardless of

ownership; b) connected to the University's network; and/or c) that is creating, accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.

F. **Mobile Device** – A portable, handheld electronic computing device that performs similar functions as a Workstation (e.g. iPhone, Android phone, Windows phone, Blackberry, Android tablet, iPad, Windows tablet, etc.).

G. **Server** – Hardware and software, and/or Workstation used to provide information and/or services to multiple Users.

H. **Workstation** - An electronic computing device, terminal, or any other device that performs as a general-purpose computer equipped with a microprocessor and designed to run commercial software (such as a word processing application or Internet browser) for an individual User (e.g. laptop, desktop computer, PC, Mac, etc.).

III. Rule

A. Data Classification

1. University electronic data must be classified according to the Data Classification Model described in this Rule, and shall be continually evaluated to determine the appropriate classification. The Data Classification Model will be used to determine the appropriate data classification for data created, maintained, processed, or transmitted using IT Resources, Information Systems, and Electronic Resources across the University. Under this Model data will be classified in accordance with external regulatory, internal regulatory, and other contractual requirements. This data classification model in no way supersedes any state or federal government classifications.

2. These data classifications apply to electronic data that University owns or has custody of, wherever it may be stored. This may include 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. This data classification methodology in no way supersedes any state or federal government classifications or other contractual classifications.

3. When a specific set of date 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 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 data breach notification requirements	Protection of data is required by the Data Steward or other confidentiality agreement	Protection of data is at the discretion of the Data Steward
Access	Only authorized individuals with approved access, signed confidentiality agreements, and a	Only authorized individuals with approved access and a business need to know	University of Utah affiliates and general public within the confines of the law

	business need to know		
Data Types	• Personally Identifiable Information (PII) • Protected Health Information (PHI) • Payment Card Industry (PCI) • Financial information • Donor information	• Intellectual Property • designated Non-Public Academic Activity Information (DNPAAI) • Employee information • Student information • Current litigation materials • 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. the Department of Homeland Security (DHS), and is defined by DHS as "any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." PII must be protected prior to release in accordance with the Utah Government Records Access Management Act (GRAMA) or other disclosures required by law.

    b. PII includes but is not limited to the following:

        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

            F. Fingerprints or other biometric identifiers

        ii. Full name in combination with:

            A. Mother's maiden name

            B. Date of birth

            C. Last 4 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 that relates to the health or health care of an individual, and specifically includes but is not limited to the following:

      i. Any PII field in combination with the following medical modifiers:

         A. Diagnosis or ICD code

         B. Treatment or CPT code

         C. Provider name or number

         D. DEA number

         E. Physician name

         F. Treatment date

         G. Patient notes

         H. Psychiatric notes

         I. Patient photos

         J. Radiology images

3. Payment Card Industry (PCI) Data

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

i. Cardholder Data:

A. Primary Account Number (PAN)

B. Cardholder name

C. Service code

D. Expiration date

ii. Sensitive Authentication Data:

A. Full magnetic stripe data

B. CAV2/CVC2/CVV2/CID

C. PIN/PINBlock

4. Financial Information

a. Financial information is governed by the Financial Accounting Standards Board (FASB) and 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 must 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 information about financial asset donations that has a stated purpose at the bequest of the donor, and includes but is not limited to:

i. Donor's full name

ii. Donor contact information

iii. Securities donated

iv. Real estate donations

v. Planned giving arrangements

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 student), which the individual has, through approved procedures, specifically designated information that is not intended to be made available to the general public. Such information may be reported to University administrators for purposes of evaluation of the individual's performance, and shared with limited sets of other persons for purposes of furthering the academic activity, but in accord with the requirements and limitations of Policy [####] is considered as sensitive information, not intended to be made accessible to the general public.

i. Types of information which an individual may choose to so designate, under the terms of Policy [####] and associated Regulations, may include, for example:

   A. Academic research or teaching activities involving use of live animal research subjects, or other controversial matters,

   B. Academic research or teaching activities involving control of hazardous materials, or technology which presents a high risk of harm to persons or property

   C. Academic service activities involving affiliation with an organization which, if made known to the general public may result in risk of bodily or other harm to the individual.

ii. As more fully described in Policy [####] and associated Regulations, an individual wishing to designate specified information as intended to be non-public does 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 for each submitted set of information whether it is to be made accessible to the general public as part of the Faculty Profile published by the University regarding that individual, or intended to not be made accessible

   {Drafting note: it will explained in the companion Policy [####], to be developed in a later phase of this project, that even for information which an individual has designated as non-public, 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-- as for example the Utah Government Records Access Management Act}.

3. Employee Information

    a. Employee information is managed by Human Resources, protected by state or federal laws and regulations, including regulations of the United States Department of Labor, and is data directly associated with an employee or applicant for employment, which must 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

        v. Salary

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

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

5. Current Litigation Materials

   a. Current litigation materials are electronically stored information that pertain to a current litigation hold implemented by the University's Office of General Counsel. These include but are limited to:

      i. Word, Excel, PowerPoint documents

      ii. PDF documents

      iii. Email

      iv. Calendar items

      v. Electronic voice mail

      vi. USB drives

6. Contracts

   a. Electronic copies of agreements, to which the University is a party, creating obligations enforceable by law.

7. Physical building and utilities detail documentation, including images {explanation of Building Info still to be developed}

E. Data Encryption

All data encryption decisions must be formally documented, and shall be considered in the context of the data at rest and data in motion. IT professionals

must work in cooperation with the Information Security Office to determine encryption requirements, as these requirements may change due to the University's technology equipment, an emerging threat, and/or in response to regulatory requirements.

1. Data At Rest Requirements

    a. For University data stored outside the University:

        i. Restricted data: encryption is required in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.

        ii. Sensitive data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.

        iii. Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.

    b. For University data stored within the University:

        i. Restricted 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.

        ii. Restricted 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.

        iii. Sensitive data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.

        iv. Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.

2. Data In Motion Requirements:

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

        i. Restricted data: encryption is required in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance

        ii. Sensitive data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.

        iii. Public Data: encryption is optional and should be in accordance with the Data Steward's requirements.

    b. For University data transmitted within the University network:

        i. Restricted data: encryption is recommended in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance.

        ii. Sensitive data: encryption is strongly recommended and should be in accordance with the Data Steward's requirements.

        iii. Public data: encryption is encouraged and should be in accordance with the Data Steward's requirements.

F. Information Security Program Data Retention

1. Information Security Program Documentation

    a. The Chief Information Security Officer shall be responsible for maintaining all information security program documentation. This documentation shall be made available for all University workforce members and Users.

    b. The Chief Information Security Officer shall be responsible for ensuring that any action, activity, or designation required by the information security

program documentation is maintained in paper and/or electronic form. All such documentation shall be maintained as specifically required.

2. Information Security Program Documentation Retention

   a. All information security program documentation, and all revisions of information security program documentation, shall be retained for six (6) years from the date of its implementation.

   b. No information security program documentation shall be destroyed before consultation with the Office of General Counsel, Chief Compliance Officer, and the Chief Information Security Officer.

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information--the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

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

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

D. Forms

E. Other related resources

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

VI. Contacts

A. The designated contact Officials for this Policy are:

1. Policy Owner (primary contact person for questions and advice): Chief Information Security Officer, 801-213-3397

2. Policy Officer; Chief Information Officer, 801-581-3100

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases..."

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... .[and] bears the responsibility for determining -requirements of particular Policies... ." University Rule 1-001-III-B & E

VII. History

A. Current version: Revision 1, effective date: April 4, 2016

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Background information for this version