Data Governance & Classification Policy 9.1.1.A Data Classification and Data Types

Data Classification and Data Types

The university utilizes various data types. Data types with similar levels of risk sensitivity are grouped together into data classifications. Four data classifications are used by the university: **Export Controlled**, **Restricted**, **Controlled** and **Public**. The Data Trustee is ultimately responsible for deciding how to classify their data (see Roles and Responsibilities for list of Data Trustees and additional information).

On a periodic basis, it is important to re-evaluate the classification of university data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the university. This evaluation must be conducted by the appropriate Data Trustee. Conducting an evaluation on an annual basis is recommended; however, the Data Trustee must determine the frequency that is most appropriate based on need. If a Data Trustee determines that the classification of a certain data set has changed, an analysis of security controls must be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they must be corrected in a timely manner, commensurate with the level of risk presented by the gaps. If you have any questions related to classification of data, please contact the IT@UC Office of Information Security (OIS) at 513-558-ISEC (4732) or infosec@uc.edu.

Data Types

The University of Cincinnati has defined four Data Types and created a data classification for each university data: **Export Controlled**, **Restricted**, **Controlled** and **Public**. The following sections will define these data and provide examples of each type:

Export Controlled

As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology. This data is labeled Export Controlled. Trustees, Stewards, Custodians and Users of Export Controlled data must follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. Trustees, Stewards and Custodians of systems that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards.

The following table contains examples of Export Controlled data. Please note this is a list of common examples and not an exhaustive listing. Please work with the Export Controls Office if you require additional assistance.

Export Controlled
• Any information labelled Export Controlled or ITAR USML Category or EAR CCL ECCN or any DoD Distribution Statement other than A. • Information or technology subject to the authorization requirements of 10 CFR part 810, or Restricted data as defined in section 11 y. of the Atomic Energy Act of 1954, as amended, or of other information, data, or technology the release of which is controlled under the Atomic Energy Act and regulations therein. • Proprietary or 3rd Party information not in the public domain or being published, must be protected until an export classification determination is complete.

Restricted

Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all safeguards for Controlled data plus additional safeguards identified for Restricted data. High levels of security safeguards must be applied to Restricted data.

The following table contains examples of Restricted data, please note this is a list of common examples and not an exhaustive listing. Please work with the Data Trustee and OIS if you require additional assistance classifying data.

Restricted
Personally Identifiable Information Personally Identifiable Information (PII) that consists of an individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements: • Social Security number or partial Social Security number • Driver's license number • State identification card number • Passport number

Restricted - continued

- United States Permanent Resident Card or similar identification
- SSID – Statewide Student Identifier
- Financial account number
- Credit card number
- Debit card number
- Electronically stored biometric information

HIPAA

For more HIPAA information please view the university's HIPAA Policy.

- Patient names
- Street address, city, county, zip code
- Dates (except year) related to an individual e.g. clinical encounters
- E-mail, URLs, & IP addresses
- Social Security numbers or partial Social Security numbers
- Account/Medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle id's & serial numbers
- Device id's & serial numbers
- Biometric identifiers
- Full face images associated with HIPAA records
- Payment guarantor's information
- Any PHI not de-identified per the Safe Harbor De-Identification method listed in the university HIPAA Policy

Employee Information

- Social Security number or partial Social Security number
- Home address or personal contact information
- Benefits information
- Worker's compensation or disability claims

Legal Information

- All data in the Office of the General Counsel unless otherwise classified by the General Counsel

FERPA Restricted Non-Directory Data

- Transcripts, defined as any cumulative listing of a student’s grades
- Student financial services information
- Credit card numbers/Bank account numbers/Debit cards numbers
- Birth name is Restricted if a preferred name is selected
- Wire transfer information
- Payment history
- Financial Aid/Grant information
- Student tuition bills

Restricted - continued

General Data Protection Regulation: Personal Data

Applies to European Union residents, permanent or temporary, regardless of citizenship. Includes any information relating to an identified or identifiable person (data subject). Applies to all individuals regardless of student or employee status. Applies to all data that alone or in combination identifies a person directly or indirectly including but not limited to:

- An identification number such as a passport, national ID, or driver's license number
- Location data such as home address
- An online identifier such as email or IP address
- Any data specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person such as a photo, social media profile, political opinions, or religious beliefs

Donor Information

- Name
- Credit card numbers/Debit card numbers
- Bank account numbers
- Social Security numbers or partial Social Security numbers
- Amount/what donated
- Telephone/Fax numbers
- Employment information
- Family information(spouse(s)/children/grandchildren)
- Medical history

Housing Data

- Name; Credit rating/history
- Financial worth; Income levels and sources, etc.

Research Information

- Human subject information
- Lab animal care information
- Proprietary data as classified by an industry sponsor
- UC proprietary or 3rd party information
- Not in the public domain or information being published

Business Information

- Credit card numbers; Bank account information
- Proprietary data covered by confidentiality or non-disclosure agreements such as but not limited to: Contracts or proposals; project specifications; proprietary company data; models, figures, illustrations.
- Purchasing card (P-card) numbers

Restricted - continued

- Social Security or other taxpayer ID numbers
- Contract information (between UC and third parties)

ISO Number

- Bearcat Card
- Campus Recreation Center
- Parking and Housing
- Administration and operation of the Card Access/Badge system including creating ISO number replacement for lost badges
- Contract information (between UC and third parties)
- Remote student printing service
- Swipe UC IDs for Patron record checkouts in the libraries
- Campus dining and meal plans
- UC Bookstore
- Time clock in/out
- GradesFirst
- Tutor Trac
- DAAP System
- eProfessional
- Blackboard
- UCFileSpace
- Data Warehouse
- Identity Management

Miscellaneous Restricted Data

- Data that the university classifies or determines to be highly sensitive

Controlled

Data is classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as Export Controlled, Restricted or Public data must be treated as Controlled data. A reasonable level of security safeguards must be applied to controlled data.

The following table contains examples of Controlled data, please note this is a list of common examples and not an exhaustive listing. Please work with the Data Trustee and OIS if you require additional assistance classifying data.

Controlled

FERPA Controlled Non-Directory Data

- Graded work, grade book, etc.
- Name; Birth name is controlled if no preferred name is selected
- Date of birth
- Place of birth
- Directory address and phone number
- Electronic mail address
- Mailing address
- Campus office address (for graduate students)
- Secondary mailing or permanent address
- Residence assignment and room or apartment number
- Dates of attendance, i.e. specific semesters of registration
- Enrollment status
- UC degree(s) awarded and date(s)
- Major(s), minor(s) and field(s)
- University degree honors
- Institution attended immediately prior to UC
- ID card photographs for university classroom use
- UCID (unique identifier for all students)
- College and class

FERPA Controlled Directory Data

Note that the following data may ordinarily be revealed by the university for Directory Information Purposes without student consent unless the student designates otherwise. If the student designates otherwise, then the following data elements must be treated as Controlled data.

- Name; Birth name is controlled if no preferred name is selected
- Directory address and phone number
- Dates of attendance, i.e. specific quarters or semesters of registration
- Enrollment status, i.e. college, class (frosh, sophomore, etc...)
- UC degree(s) awarded and date(s)
- College and class
- Major(s), minor(s) and field(s) of study
- University degree honors and awards

Management Data

- Faculty and staff reviews and performance evaluations

Controlled - continued
Miscellaneous Controlled Data • Data from research germane to intellectual property that is not categorized as Restricted • Data whose integrity must be maintained • Other data that must be protected but is not classified as Restricted

Public

Data that is readily available to the public. This data requires no confidentiality or integrity protection.

Related Links

Data Governance & Classification Policy

Contact Information

IT@UC Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

History

Issued: 07/01/2009
Revised: 05/30/2014
Revised: 01/25/2017
Revised: 10/25/2017
Revised: 09/26/2018
Revised: 11/16/2018
Revised: 09/25/2019