Data Stewardship Responsibilities, Guidelines, and Classification Policy	6-014 TECHNOLOGY SERVICES December 2019

PURPOSE

1.01 The purpose of this policy is to establish data classification guidelines and minimum requirements to be followed when identifying applicable data and to clarify the data classification responsibilities of data stewards, data custodians, access custodians, and data users.

SCOPE

2.01 This policy applies to all data created, collected, stored, processed, or transmitted via institutional resources, in electronic or non-electronic formats.

2.02 The Vice President of Fiscal Services or his/her designee, will have oversight responsibility for institutional provisions that define data, data classification guidelines, data standards, enforcement mechanisms, and ongoing maintenance of this policy and related explanatory documents.

2.03 Individual schools and units within the institution may define conditions of use for information resources under their control. These statements must be consistent with this overall policy and may provide additional detail, guidelines, and restrictions. Such policies may not relax or subtract from this policy or any institution approved standards.

2.04 This policy applies to all members of the OSUIT community who have been granted access to institutional data.

DEFINITIONS

3.01 **Data:** Information collections in electronic format including but not limited to databases, spreadsheets, and email, or in non-electronic format including but not limited to paper files, publications, and hardcopy research. Data are information or knowledge concerning a particular fact or circumstance, gained via study, communication, research, or instruction.

3.02 **Data Steward:** An individual with the responsibility for coordinating the implementation of this policy through the establishment of definitions of the data sets available for access and the development of policies and access procedures for those data sets.

3.03 **Data Custodian:** The authoritative head of the respective unit, or a principle investigator or project director; those who manage and protect data and are responsible for operations relating to the information.

3.04 **Access Custodian:** An individual or individuals responsible for implementing the controls identified and specified by this policy and the Data Custodian. Appropriate processing, storage, and transmittal protocols of information are under the purview of the Access Custodian.

3.05 **Data User:** Individuals authorized to access, create, or alter information under the scope of this policy.

3.06 **Conditions of Use:** For the purposes of this document, the restrictions around allowed use of information or data by Data Users or the acceptable circumstances under which Data Users encounter data.

3.07 **FERPA** (Family Educational Rights and Privacy Act): Regulates student education records such as class lists, grade rosters, records of advising sessions, grades, and financial aid applications.

3.08 **HIPAA** (Health Information Portability and Accountability Act): Regulates certain health information such as health records, patient treatment information, and health insurance billing information.

3.09 **PII** (Personally Identifiable Information): Social security numbers, credit card numbers, driver's license numbers, and bank account numbers.

3.10 **GLBA** (Gramm-Leach-Bliley/Financial Services Modernization Act): Regulates Bursar records.

3.11 **PCI** (Payment Card Industry): Regulates information dealing with debit, credit, prepaid, e-commerce, ATM, and POS cards such as credit card numbers, names, and other information used for payment processing.

3.12 **DMCA** (Digital Millennium Copyright Act): Regulates the use of copyrighted protected material including but not limited to audio, video, software, and documents.

3.13 **U.S. Export Controlled Information:** Any information that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State.

POLICY

4.01 Data for which OSUIT is to be held responsible shall be assigned one of the following classification levels:

Confidential/Regulated—Data protected specifically by federal law, state law, or OSUIT policies and procedures including but not limited to FERPA, GLBA, HIPAA, PCI, DMCA, PII, and U.S. Export Controlled Information. This includes information which requires protection under contractual agreements such as non-disclosure agreements, various memoranda of understanding, and granting or funding agency agreements.

Internal—Data available for release under appropriate mechanisms in a controlled and lawful manner.

Public—Publicly available data without requirements for confidentiality, integrity, or availability.

4.02 Aggregations of information shall be assigned at the highest level of the most restrictive classification requirements of any individual piece of information contained in the aggregate.

RESPONSIBILITIES

5.01 Data Stewards are responsible for:
- Developing access control procedures consistent with this university data policy.
- Coordinating implementation of Data Classification Policy for a school or unit.

5.02 Data Custodians are responsible for:
- Appropriately classifying data.
- Ensuring access custodians are implementing appropriate and thorough controls for securing data according to the expectations of the data classification level assigned.
- Developing means of educating data users on proper security procedures for the data they protect

5.03 Access Custodians are responsible for:
- Implementing the controls specified by policy, standards, guidelines, and Data Custodians, by administering physical and logical safeguards and monitoring mechanisms for the information resources under their control.
- Appropriately and thoroughly educating users of data on the data classification level and expected measures of security associated with that level.
- Releasing data to individuals only if they have a legitimate need to know.

5.04 Data Users are responsible for complying with:

- All appropriate use policies and procedures.
- All operational requirements associated with this policy.

5.05 Users who fall within the scope of this document are responsible for reporting suspected violations of this policy to their direct supervisor or the institutional department associated with the data involved immediately.

APPROPRIATE DATA USE

6.01 Unauthorized access, manipulation, release, or change of data in ways related to the examples below are prohibited.

6.02 Access, manipulation, release, or change of data is authorized if required to fulfill assigned university duties.

6.03 The individual with the legitimate need to know must remain mindful of any university policies or federal, state, or local laws specifically related to the accessing, handling, and disclosure of that data and viewing. Access to data must serve specific university need and not be broader than necessary to perform an individual's job function. Data access must be based on an individual's authorized permissions. In order to not compromise the integrity of university data, sharing of passwords is not allowed.

6.04 Failure to comply with data classification policies and classification standards can result in revocation of access, retraining on data security, notification of supervisors, loss of funding, lawsuits, suspension, and possible termination of employment.

Approved: August 2017
Revised: December 2019