Oklahoma State University Policy and Procedures

DATA STEWARDSHIP: DATA CLASSIFICATION POLICY, RESPONSIBILITIES AND GUIDELINES	3-0602 ADMINISTRATION & FINANCE Information Technology October 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 This policy applies equally to all information assets and technology resources.

2.03 This policy assigns responsibilities to individuals or individual units within the institution tasked with stewardship, custodianship, or other responsibilities regarding information resources under their control.

2.04 This policy applies to all members of the Oklahoma State University (OSU) community who have been granted access to University data, whether students, faculty, staff, or authorized third-party users.

DEFINITIONS

3.01 Access Custodian – an individual or individuals responsible for implementing the controls identified and/or specified by this policy and the Data Custodian. Appropriate processing, storage, and transmittal protocols of information are under the purview of the Access Custodian.

3.02 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.

3.03 Data – information collections, either electronic (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University's mission.

3.04 Data Custodian – the authoritative head of the respective College, Division or Department, or a Principal Investigator or Project Director; those who manage and protect data and are responsible for operations relating to the information.

3.05 Data Stewards – 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/or access procedures for those data sets or otherwise defined within this document.

3.06 Data User – an individual, whether authorized or not, who makes use of, accesses, creates, or alters information under the scope of this policy.

3.07 Information assets – any University-owned, -leased, -protected, or otherwise authorized information or data.

3.08 Information systems – any resource or equipment used for accessing or for controlling access of information assets.

3.09 Information technology resources – technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching, or other purposes.

POLICY

4.01 Data Classification – data for which OSU is responsible shall be assigned one of the following classifications:

- Confidential/Regulated – data protected specifically by federal, state, or OSU rules and regulations (e.g. FERPA, Gramm-Leach-Bliley, HIPAA, PCI-DSS, U.S Export Controlled information, Board of Regents policies, etc.) and/or data which includes information which requires protection under contractual agreements (e.g., Non-Disclosure Agreements, various Memoranda of Understanding, Granting or Funding Agency Agreements, etc.)
- Internal – data available for release under appropriate mechanisms in a controlled and lawful manner, or
- Public – data available without requirements for confidentiality, integrity, or availability.

4.02 Classification Expectations

A. 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.

B. Social Security Numbers (SSNs) will be treated as confidential/regulated data. Security controls for SSNs will include, but not be limited to, authentication for access, masking or encryption for transmission, and encryption for storage.

C. Collection and use of confidential/regulated data is only permitted as authorized by law or administrative exception. Data Users will exhibit due diligence to secure collection, storage, processing, or transmission of confidential/regulated data. Confidential/regulated data will not be accessed without legitimate business purpose.

4.03 Personnel Responsibilities

A. Policy Oversight

The highest administrative and financial provisions figure of authority on the OSU campus, such as the Senior Vice President for Administration and Finance or other Vice Presidential position or his/her designee, will have oversight responsibility for:

1. institutional provisions which define data;

2. data classification guidelines and standards;

3. enforcement mechanisms; and

4. ongoing maintenance of this policy and related explanatory documents.

B. Conditions of Use

Individual units within the institution define ‘conditions of use’ for information resources under their control.

1. These statements must be consistent with this overall policy and may provide additional detail, guidelines, and/or restrictions.

2. Such policies may not relax or subtract from this policy or any institution approved standards.

C. Data Stewards

The Data Steward’s role is to act with proper and appropriate levels of responsibility within a trust relationship regarding institutional data. This role’s responsibilities will reflect OSU’s values regarding both the free exchange of information as an academic institution, as well as a protector of certain information.

1. There will be eight administrative functional areas of OSU, with respective data stewards, as follows:

Administration & Finance	Sr. Vice President for Administration & Finance
Admissions/Recruitment	VP Enrollment and Brand Management
Cooperative Extension and Agricultural Experiment Station	VP of Agriculture
Facilities Management	Chief Facilities Officer
Human Resources	Assistant Chief Human Resources Officer
Information Technology	Chief Information Officer

Research Administration	Vice President for Research
Registration/Transcripts	Provost & Sr. Vice President
Student Affairs	Vice President for Student Affairs

2. Data Stewards will be responsible for:
    a. Developing access control procedures, in accordance with this University data policy; and

    b. Coordinating implementation of the Data Stewardship Policy for administrative areas.

3. Delegation of Data Steward Responsibilities
    a. Data Stewards may delegate a portion, but not all, of their Stewardship responsibilities to proper delegates with appropriate levels of operation and/or authority to receive those delegated responsibilities.

    b. Delegation of responsibilities does not absolve Stewards of the inherent trust relationship regarding data in which their institutional/operational interests reside.

D. Data Custodians
Data custodians are responsible for:
1. appropriately classifying data;

2. ensuring Access Custodians are implementing appropriate and thorough controls for securing data according to the expectations of the data classification level assigned; and

3. developing means of educating data users on proper security procedures for the data they protect.

E. Access Custodians
1. Access custodians are responsible for:
    a. 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; and

    b. appropriately and thoroughly educating users of data on the data classification level and expected measures of security associated with that level.

2. Access Custodians may only release data to individuals with a legitimate interest in the data.

F. In certain situations, the same individual may hold the roles or responsibilities of Data Steward, Data Custodian, and/or Access Custodian.

G. Data Users

1. Data users are responsible for complying with:
    a. all appropriate use policies and procedures; and

    b. all operational requirements associated with this policy.

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

4.04 Appropriate Data Use

Unauthorized access or change to, or manipulation or release of, data in the following ways are prohibited:

A. Access, manipulate, release, or change of data is authorized if required to fulfill assigned University duties.

B. The individual with the legitimate interest must remain mindful of any University policies or federal, State, or local laws specifically related to the accessing, handling and/or disclosure of that data.
Note: These examples are illustrative, not exhaustive.

1. Do not change data about yourself or others for other than usual business purposes.

2. Do not use information (even if authorized to access it) to support actions by which individuals might profit or benefit (e.g., a change in salary, title, or band level; a better grade in a course).

3. Do not disclose information about individuals without prior supervisor authorization.

4. Do not engage in what might be termed “administrative voyeurism” (e.g., tracking the pattern of salary raises; determining the source and/or destination of telephone calls or Internet protocol addresses; exploring race and ethnicity indicators; looking up grades), unless authorized to conduct such analyses.

5. Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access (e.g., providing a university-wide data set of human resource information to a coworker who only has approved access to a single human resource department), unless authorized.

6. Do not facilitate another's illegal or improper access to OSU’s administrative systems or compromise the integrity of the systems data by sharing your passwords or other information.

4.05 Non-Compliance

Failure to comply with data classification policies and classification standards can result in immediate revocation of privileges to use the University's computing resources, revocation of access, required re-training on data security, notification of supervisors, loss of funding, lawsuits, suspension, and possible termination of employment.

Violations of this policy may result in disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

PROCEDURAL GUIDANCE

5.01 Procedural Questions

For questions regarding procedural application of this policy:

Subject	Contact
Policy Clarification	OSU IT Information Security office

For data stewardship and custodianship specific questions:

Subject	Contact
Administration & Finance	Office of Vice President for Administration & Finance
Admissions (Undergrad)	Office of Undergraduate Admissions
Admissions (Graduate)	Graduate College
Cooperative Extension and Agricultural Experiment Station	Office of Vice President of Agriculture
Financial Information	Financial Information Management
Facilities Management	Facilities Management Administration
Human Resources	Human Resources Information Management
Institutional Research	Institutional Research & Information Management
Information Technology	Office of the CIO
International Student Information	International Students & Scholars Office
Research Administration	Office of the Vice President of Research
Student Information	Office of the Registrar
Student Affairs	Office of the Vice President for Student Affairs

5.02 Regulated Data Chart

This chart is a companion to the policy and provides guidance information on what data may be stored on certain applications. This is not a comprehensive explanation of appropriate use for data; as allowed use is determined by those parties deemed responsible by the policy.

How to interpret the Regulated Data Chart:
● **Use Permitted**: No technical, policy, or contractual issues exist that prohibit use of this data type with this service. Sending, storing, or sharing the regulated data type is authorized if the data steward and department/unit policies permit to do so.
⊖ **Use Restricted**: Use of this service with the regulated data type is restricted and approval is required.
✕ **Use Prohibited**: Use of this service with the regulated data type is prohibited. Do not use this service to send, store or share the regulated data type.

Application	**FERPA**	***HIPAA (ePHI)**	**Personal Identifiers**	**GLBA**	**Human Subjects**	**PCI**	**Restricted Research Data**	**GDPR**
Email								
Broadcast Mailing Systems	✕	✕	✕	✕	✕	✕	⊖	✕
Cowboy Mail	●	⊖	✕	✕	✕	✕	●	●
Office 365	●	⊖	⊖	✕	✕	✕	●	●
Orange Mail	●	✕	✕	✕	✕	✕	●	●
Storage Devices								
Cowboy Mail SkyDrive	●	⊖	⊖	✕	⊖	✕	⊖	●
Application	**FERPA**	***HIPAA (ePHI)**	**Personal Identifiers**	**GLBA**	**Human Subjects**	**PCI**	**Restricted Research Data**	**GDPR**
Department Network Drive (G	●	✕	⊖	✕	⊖	✕	●	●
Orange Mail Google Doc	⊖	✕	⊖	✕	⊖	✕	⊖	⊖
Personal Network Drive (H)	●	⊖	⊖	✕	⊖	✕	●	●
SecureDrive	●	⊖	⊖	✕	⊖	✕	●	●

Sub Department Network Drive (I)	●	✕	⊖	✕	⊖	✕	●	●
Campus wide Network Drive (J)	✕	✕	✕	✕	✕	✕	✕	✕
Document Services								
Document Imaging	⊖	⊖	⊖	⊖	⊖	✕	⊖	⊖
ePrint	⊖	⊖	⊖	✕	✕	✕	✕	⊖
Remote Printing	✕	✕	✕	✕	✕	✕	✕	✕
Virtualization								
Online Classroom Services (D2L, Canvas, etc.)	●	✕	✕	✕	●	✕	●	●
Online Classroom Community Sites	✕	✕	✕	✕	⊖	✕	⊖	✕
IT Virtual Labs	✕	✕	✕	✕	⊖	✕	⊖	✕
IT Virtual SAS	✕	✕	✕	✕	⊖	✕	⊖	✕
MSIS Virtual Desktop	✕	✕	✕	✕	⊖	✕	⊖	✕
Real Audio	✕	✕	✕	✕	⊖	✕	⊖	✕
Support								
iSupport	✕	✕	✕	✕	✕	✕	✕	✕
TurnItIn	✕	✕	✕	✕	⊖	✕	⊖	✕
Database Services								
MS SQL	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
Application	**FERPA**	***HIPAA (ePHI)**	**Personal Identifiers**	**GLBA**	**Human Subjects**	**PCI**	**Restricted Research Data**	**GDPR**
MySQL	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
Oracle	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
Online Collaboration								
Drupal	✕	✕	✕	✕	✕	✕	⊖	✕
Omni	✕	✕	✕	✕	✕	✕	⊖	✕
Joomla	✕	✕	✕	✕	✕	✕	⊖	✕
SharePoint	⊖	⊖	⊖	✕	⊖	✕	⊖	⊖
WebDAV	✕	✕	✕	✕	✕	✕	⊖	✕

Communication								
Jabber	⊖	✗	✗	✗	⊖	✗	⊖	⊖
MS Lync	⊖	✗	✗	✗	⊖	✗	⊖	⊖
MS Skype	⊖	✗	✗	✗	⊖	✗	⊖	⊖
VOIP Phone Services	⊖	✗	✗	✗	⊖	✗	⊖	⊖

FERPA (Family Educational Rights and Privacy Act): Education records. Examples: Class lists, grade rosters, records of advising sessions, grades, financial aid applications.

HIPAA (Health Information Portability and Accountability Act) / **ePHI** (Electronic Protected Health Information): Certain health information. Examples: Health records, patient treatment information, health insurance billing information, health benefits information. *The OSU A&M Privacy Official and OSU IT Security department must be informed of **any** storage and use of ePHI or “HIPAA data”.

Personal Identifiers: Data items which, when stored or used with other information, can identify a unique individual. Examples: Social Security Numbers, driver’s license numbers and bank account numbers.

GLBA (Gramm-Leach-Bliley/Financial Services Modernization Act): Bursar or Financial Aid records.

Human Subjects: Information that reveals or can be associated with the identities of people who serve as research subjects. Examples: names, fingerprints, full-face photos, a videotaped conversation or information from a survey filled out by an individual.

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

Restricted Research Data: Research data sets: Example: Census data and student surveys
DMCA (Digital Millennium Copyright Act): Copyrighted protected material. Examples: audio, video, software, and documents. See OSU *Intellectual Property* Policy 1-0202

GDPR (General Data Protection Regulation): Personal data of EU or European Economic Area citizens or individual personal data transferred from within to outside the EU and EEA areas. Example: an individual EU citizen’s personal data provided to the University

Approved:
Staff Advisory Council, December 2019
Faculty Council, January 2020
Council of Deans, February 2020
E-Team, April 2020
Board of Regents, April 2020