OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

860 - DATA MANAGEMENT AND INFORMATION SECURITY

SUBJECT:	DATA MANAGEMENT AND INFORMATION SECURITY
NUMBER:	860
AUTHORIZING BODY:	STRATEGY COUNCIL/BOARD OF TRUSTEES
RESPONSIBLE OFFICE:	CHIEF OF STAFF
DATE ISSUED:	MARCH 2005
LAST UPDATE:	APRIL 2021

RATIONALE: To provide guidelines with regard to the responsibility of every Oakland University (University) employee who accesses Data and information in electronic formats to provide for the security of that Data. Unauthorized access to such information may have many severe negative consequences, including adversely affecting the reputation of the University. The use of Mobile Computing Devices, electronic file exchanges, and the growing use of cloud service providers increase the vulnerability of University Electronic Data and information assets. As new technologies are developed and implemented, and as new laws covering Data security emerge, issues multiply around Data management and security.

POLICY: Electronic Data are important University assets that must be protected by appropriate safeguards and managed with respect to Data stewardship. This policy defines the required Electronic Data management environment and classifications of data and assigns responsibility for ensuring Data and information privacy and security at each level of access and control.

SCOPE AND APPLICABILITY: This policy applies to all University personnel and affiliated users with access to University Data.

DEFINITIONS:

Affiliated Users: Vendors and guests who have a relationship to OU and need access to university systems.

Application: A computer software program run on a computer for the purpose of providing a business/academic/social function.

Cloud: An on-demand availability, geographically dispersed infrastructure of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the end user. Clouds may be limited to a single organization (Private Cloud), or be available to many organizations (Public Cloud). Cloud-computing providers offer their "services" according to three standard models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Confidential Data: Data that are specifically restricted from open disclosure to the public by law are classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Confidential Data include, but are not limited to:

1. Student Data protected by the Family Educational Rights and Privacy Act (FERPA), including personal identification Data such as Social Security Number, student numbers such as Grizzly IDs, and other Data not classified as directory information under FERPA.;

2. Medical Data, such as Electronic Protected Health Information and Data protected by the Health Insurance Portability and Accountability Act (HIPAA);

3. Research. Only research data and information within the following broad categories is to be considered Confidential Data:
    a. Classified Research
    b. Activity that is covered by a fully executed non-disclosure agreement (NDA);
    c. Information, data, etc., that is proprietary or confidential (whether it belongs to an OU investigator or an outside collaborator), regardless of whether it is subject to an NDA;
    d. Information that a sponsor deems to be confidential;
    e. Information or data that is required to be deemed confidential by state or federal law (e.g., personally identifying information about research subjects, HIPAA or FERPA protected information, etc.); and

f. Information related to an allegation or investigation into research misconduct.

All other research data and information, including grant applications and proposals, drafts and working papers for patent applications or research publications, and de-identified research Data, shall be considered Operation Critical Data.

All research and proposal information that is transmitted to/from, or held on, OU's electronic research administration platform (Cayuse) is encrypted using 2048-bit SSL and/or IPSEC tunnels. Information within the Cayuse platform is only available on a need-to-know basis and requires an active OU NetID and password for authentication.

4. Information access security, such as login passwords, Personal Identification Numbers (PINS), logs with personally identifiable Data, digitized signatures, and encryption keys;

5. Primary account numbers, cardholder Data, credit card numbers, payment card information, banking information, employer or taxpayer identification number, demand deposit account number, savings account number, financial transaction device account number, account password, stock or other security certificate or account number (such as Data protected by the Payment Card Industry Data Security Standard);

6. Personnel file, including Social Security Numbers;

7. Library records (such as covered by the Michigan Library Privacy Act 455); and

8. Drivers license numbers, state personal identification card numbers, Social Security Numbers, employee identification numbers, government passport numbers, and other personal information that is protected from disclosure by state and federal identity theft laws and regulations including without limitation the Michigan Identity Theft Protection Act (MCL 445.61 et. seq.).

Data Classifications: All Electronic Data covered by this policy are assigned one of three classifications:

1. Confidential

2. Operation Critical

3. Unrestricted

Data Custodian: Persons or departments providing operational support for an information system and having responsibility for implementing the Data Maintenance and Control Method defined by the Data Steward.

Data Maintenance and Control Method: The process defined and approved by the Data Steward to handle the following tasks:

1. Definition of access controls with assigned access, privilege enablement, and documented management approval, based on job functions and requirements.

2. Identification of valid Data sources

3. Acceptable methods for receiving Data from identified sources

4. Process for the verification of received Data

5. Rules, standards and guidelines for the entry of new Data, change of existing Data or deletion of Data

6. Rules, standards and guidelines for controlled access to Data

7. Process for Data integrity verification

8. Acceptable methods for distributing, releasing, sharing, storing or transferring Data

9. Acceptable Data locations

10. Providing for the security of Confidential Data and Operation Critical Data

11. Assuring sound methods for handling, processing, security and disaster recovery of Data

12. Assuring that data are gathered, processed, shared and stored in accordance with the University privacy statement posted on https://www.oakland.edu/policies-regulations/web-privacy/

Data Steward: The persons responsible for University functions and who determine Data Maintenance and Control Methods are Data Stewards.

Electronic Data/Data: Distinct pieces of information, intentionally or unintentionally provided to the University in a variety of administrative, academic and business processes. This policy covers all Data stored on any electronic media, and within any computer systems defined as a University information technology resource under OU AP&P #890 Use of University Information Technology Resources.

Within this document, Electronic Data and Data are used interchangeably. This definition does not include course materials and intellectual property.

Mobile Computing Devices: Information technology resources (as defined in OU AP&P #890 Use of University Information Technology Resources) that may leave the general campus location. Samples of such devices include, but are not limited to, laptops, tablets, cell phones, smart phones, and other portable devices, CD/DVD R/W disks, USB devices, flash drives, etc.

Operation Critical Data: Data determined to be critical and essential to the successful operation of the University as a whole, and whose loss or corruption would cause a severe detrimental impact to continued operations. Data receiving this classification require a high level of protection against accidental distribution, exposure or destruction, and must be covered by high quality disaster recovery and business continuity measures. Data in this category include Data stored on Enterprise Systems such as Banner and Data passed through networked communications systems. Such Data may be released or shared under defined, specific procedures for disclosure, such as departmental guidelines, documented procedures or policies.

University Provided Data Systems: Information technology resources, as defined and described in OU AP&P #890 Use of University Information Technology Resources, owned by the University and used for the storage, maintenance and processing of University Data.

Unrestricted Data: Information that may be released or shared as needed. Examples are Data files for the schedule of classes or other publicly available Data such as a directory.

Usage/Data Use: Usage and Data Use are used interchangeably and are defined as gathering, viewing, storing, sharing, transferring, distributing, modifying, printing and otherwise acting to provide a Data maintenance environment.

PROCEDURES:

1. **Data Stewardship**

2. Data Stewards are expected to create, communicate and enforce Data Maintenance and Control Methods. Data Stewards are also expected to have knowledge of functions in their areas and the data and information used in support of those functions. Vice Presidents are accountable for the ultimate data management and stewardship in their respective areas of responsibility, and are the default Data Stewards for all University Data. Recognized Data Stewards are listed in the Attached Approval Table.

Data Maintenance and Control Method

Data Stewards will develop and maintain Data Maintenance and Control Methods for their assigned systems.

When authorizing and assigning access controls defined in the Data Maintenance and Control Methods involving Confidential Data and Operation Critical Data, Data Stewards will restrict user privileges to the least access necessary to perform job functions based on job role and responsibility.

If the system is a University Provided Data System, University Technology Services will provide, upon request, guidance and services for the tasks identified in the Data Maintenance and Control Method.

If the system is provided by a Public Cloud, the Data Steward must still verify that the Data Maintenance and Control Method used by the Public Cloud provider meets current University technology standards. Further, ongoing provisions for meeting current University technology and security standards must be included in the service contract.

Review of Public Cloud solutions must include University Technology Services and Office of Legal Affairs prior to final solution selection and purchase.

Us of personal equipment to conduct university business must comply with all guidance provided by UTS, and all University policies.

3. Data Custodianship

Data Custodians will use data in compliance with the established Data Maintenance and Control Method. Failure to process or handle Data in compliance with the established method for a system will be considered a violation of OU AP&P #890 Use of University Information Technology Resources, and sanctions defined in that policy may apply.

4. Data Usage

In all cases, Data provided to the University will be used in accordance with the Privacy Statement accessed from the University home page www.oakland.edu, and within the guidelines provided to those giving Data to the University (guidelines provided by the Data source).

Software solutions, including SaaS solutions, are selected to manage Data and are procured, purchased and installed in conjunction with university policies related to software (such as OU AP&P #870 Software Regulations and OU AP&P #1000 Procurement Policy).

Data will be released in accordance with University policies (such as OU AP&P #470 Release of Student Educational Records). Requests for information from external agencies (such as Freedom of Information Act requests, subpoenas, law enforcement agency requests, or any other request for Data from an external source) must be directed to the Office of Legal Affairs and processed in accordance with existing policies, particularly Authorized Use in OU AP&P #890 Use of University Information Technology Resources.

Standards for secure file transmissions, or Data exchanges, must be evaluated by University Technology Services when a system other than a University Provided Data System is selected or when a Public Cloud is utilized. Specific contract language may be required. The Office of Legal Affairs must be consulted regarding such language.

Unencrypted authorization and Data transmission are not acceptable.

Data Used in the pursuit of teaching, learning, research and administration must be managed to preserve integrity and trust. This is the responsibility of all who use Data.

Communications of Confidential Data via end-user messaging technologies (i.e., email, instant messaging, chat or other communication methods) is prohibited. UTS can validate if a particular technology is suitable for communicating Confidential Data.

5. Storing data

Data cannot be stored on a system other than a University Provided Data System without the advance permission of the Data Steward and demonstrated legitimate need.

Data should be stored in encrypted formats whenever possible. Confidential Data must be stored in encrypted formats. Encryption strategies should be reviewed with University Technology Services in advance to avoid accidental Data lockouts.

Data cannot be stored on a University-provided Computing Device unless the device is encrypted without the advance permission of the Data Steward and demonstrated legitimate need.

Data must be stored on devices and at locations approved by Data Stewards. If information technology resources (computers, printers and other items defined in OU AP&P #890 Use of University Information Technology Resources) are stored at an off-campus location, the location must be approved by Data Stewards and UTS prior to using such resources to store University Data.

New technology enables the storage of Data on fax machines, copiers, cell phones, point-of-sale devices and other electronic equipment. Data Stewards are responsible for discovery of stored Data and removal of the Data prior to release of the equipment.

When approving Mobile Computing Device Usage, Data Stewards must verify that those using Mobile Computing Devices can provide information about what Data was stored on the device (such as a copy of the last backup) in the event the device is lost or stolen.

In all cases, Data storage must comply with University retention policies. Data Usage in a Public Cloud system must have specific retention standards written in the service contract. The Office of Legal Affairs must be consulted regarding such language.

Provisions for the return of all University Data in the event of contract termination must be included in the contract, when Data are stored on a Public Cloud. The Office of Legal Affairs must be consulted regarding such language. Current security standards (such as controlled access, personal firewalls, antivirus, fully updated and patched operating systems, etc.) will be evaluated when a system other than a University Provided Data System is selected and must be covered in contract language. The Office of Legal Affairs must be consulted regarding such language.

Data stored on Mobile Computing Devices must be protected by current security standard methods (such as controlled access, firewalls, antivirus, fully updated and patched operating systems, etc.).

University standard procedures for the protection and safeguarding of Confidential Data and Operation Critical Data must be applied equally and without exception to University Provided Data Systems, Mobile Computing Devices and systems other than University Provided Data Systems, such as Public Cloud solution.

6. Systems and network data

Systems and network Data, generated through systems or network administration, logs or other system recording activities, cannot be used, or captured, gathered, analyzed or disseminated, without the advance permission of the Chief Information Officer, University Technology Services.

7. Value of data

In all cases where Data are to be processed through a Public Cloud, the following assessment must be done:

- The value of the Data must be determined in some tangible way.

- Signature approval from the Data Steward’s division vice president or appropriate party with the ability to authorize activity at the level of the value of the Data must be obtained.

8. Sanctions

Failure to follow the guidelines contained in this document will be considered inappropriate use of a University information technology resource and therefore a violation of OU AP&P #890 Use of University Information Technology Resources. Sanctions will follow the steps identified in that policy.

9. Data Security Breach Review Panel

A Data Security Breach Review Panel (Panel) comprised of the following members will be established:

- Associate Vice President and Controller
- Chief Information Officer
- Chief of Police
- Director of Campus Communications
- Registrar
- Director of Risk Management
- Office of Legal Affairs

If unauthorized access to Confidential Data is discovered, a member of the Panel must be contacted, who will then convene the Panel. This contact with the Panel must be initiated as soon as possible after the breach in order to assist the University in meeting its legal obligations, and may be initiated by the Data Steward, by the user of the Data, by the owner of a missing or stolen laptop or storage device, or by anyone who has become aware of unauthorized Data access.

Examples of potential data security breaches that require notification include, but are not limited to:

- Theft or loss of a laptop, desktop computer, or storage device used to store Confidential Data

- Unauthorized access to a Database system or hack of a University system or website.

The Panel will:

- Review the situation and assess the potential for Data exposure. It is expected that the owner of the system in question will be able to identify the Confidential Data that were stored on that system.

- Perform digital forensics necessary to assess the threat and take steps to limit the breach.

- Develop and implement a response plan to ensure the University's compliance with all legal and other obligations in regards to the breach.

RELATED POLICIES AND FORMS:

OU AP&P #212 Bankcard Information Security Requirements

OU AP&P #360 Property Management

OU AP&P #470 Release of Student Educational Records

OU AP&P #870 Software Regulations

OU AP&P #890 Use of University Information Technology Resources

OU AP&P #1000 Procurement Policy

OU AP&P #1050 Risk Management/Insurance Policies & Procedures

Data Stewards Approval Table

APPENDIX: