Data Classification and Retention Policy (ISP-08)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all faculty, staff, and contractors issued access to University IT resources and services.

Table of Contents

Introduction

The University collects data to administer its programs and execute research and learning activities. To be able to secure data, be compliant with federal and state legislation and ensure the privacy of our applicants, student, staff, and associates personal data it is necessary to classify and identify where data is being held as well as define how long we can retain certain data types.

Objective

This policy's objective is to ensure all staff and contractors are aware of their responsibilities when ingesting, creating, modifying, storing, sharing, and handling data.

Policy Statement

General

All staff, employees, contractors, consultants, temporary, and other workers at the University are responsible for exercising good, sound judgment regarding appropriate use of Personal and University data. Those handling data should also ensure they are compliant with the Privacy Policy and rules issued by the University Administrative Department.

Data Classification

Data will be classified into one of three categories based on the sensitivity of the data:

1. Public Data – Available information and data with no sensitive information present, such as course details, marketing, and new applicant packages.
2. Restricted Data - Private or Internal, sensitive information such as sales information, new course material, student results and feedback.
3. Confidential Data - Data that contains sensitive data such as directly addressable Personally Identifiable Information (PII), Bank Account Details, Salary Information, or sensitive business growth information such as acquisitions and growth plans.

Note that any medical information shall be classified and handled as required under HIPAA and medical privacy policies.

Data Labeling and Tagging

All media containing Restricted and Confidential data is to be marked as such. Emails should contain the classification in the subject line. Data should be tagged where possible, and a comment inserted into the meta data or data body. Documents should clearly define the classification on the cover-page and on each page containing such information in the header.

Data Handling and Transmission

Data and documents are to be handled as defined in the following table, as a general approach the least privilege rule should be adopted in effect this means if and individual does not need access to information to perform their functions, they should not have access.

Data Classification	Electronic Format	Hard Format
Public	No formal controls, users should use sound judgement.	No formal controls, users should use sound judgement.

Restricted	This data may be emailed between internal and external parties	A clear desk policy should be in place and all documents locked up when not in use
Confidential	Must be encrypted. You may send internally via email but not externally	A clear desk policy must be in place and all documents stored in a certified document storage cabinet

Data and Document Retention Requirements

Leading practice continues to show significant benefit, and risk reduction can be achieved through the removal and destruction of data once its usefulness has passed. As a result, data, which includes documents and records, shall be disposed of in a secure and auditable manner once the retention periods defined in Appendix A have been exceeded.

It is noted that at certain times these retention periods may need to be extended because of investigation, litigation, or legal hold – all such reasons are to be documented and reviewed quarterly to ensure they are still applicable.

Destruction of Media

Electronic Media that has come in contact with Confidential and Restricted information must either be physically destroyed or purged using secure erase software. Physical paper destruction is to be achieved by burning or shredding using a crosscut shredder. Secure erasure products and procedures will be provided by the IT department. During destruction audit artifacts are to be created that define what was destroyed by whom, how it was performed and a witness.

Data Inventory

The IT department must maintain and update manually an inventory that identifies all locations and systems where Restricted and Confidential data is stored and processed. Additionally, any data stores that handle PII data are to be identified. Data Custodians are expected to assist in this process.

Legislative Considerations

This policy takes into account all known legal requirements in the area of records retention and destruction. Legal requirements take precedence over this policy and associated procedures. Any known instances of conflict between this policy and legal requirement are to be shared with the CISO and legal counsel.

Appendix A – Data Retention Periods

This appendix defines the retention period that data and records, be they electronic or paper, be retained by the University. Past that point in time records are to be disposed of in accordance with this policy

Business Area	Record Type	Maximum Retention Max (Yr)	Notes
All	Business correspondence	7	
All	Business operations	7	
All	Routine business communication	7	
Corporate	Corporate Records (Meeting minutes)	For Ever	This includes ownership or corporate board and sub committees and governance meetings
Corporate	Articles of incorporation of similar	For Ever	
Finance	Credit Card Receipts	5	Note PCI requirements for PAN handling
Finance	Tax information and returns	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	Business expense records	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	Invoices and receivables	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	Payroll Tax records	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	Payroll records	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	Financial audits	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Finance	General Ledger and sub ledgers	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7,
Finance	Investment records	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
Corporate	Business Contracts	7	Federal, state and SOX, FDIC Bank Secrecy Act is 7
HR	Employment Applications	5	
HR	Accident Records	5	
HR	All Identifiable HR records including promotion, discipline, pay	3	From date of departure This is required for employees who are terminated FLSA is 3 years
HR	Termination and departure	3	FLSA is 3 years
IT	Architecture decisions	3	Long term value to be able to understand how evolved
IT	Operations material excluding logs	3	
IT	Test Results	3	
IT	Performance & Availability logs	3	
Student	Student Loan Data	7	
Student	Summary Results	For Ever	
Student	Academic Achievements Results Feedback etc.	5	Note start points are complex so increased from 3 to 5 to simplify retention implementation.
Student	PII other than in directory	3	
Student	Disciplinary Information	3	
Student	Attendance Records	5	
Student	Alumni Records	For Ever	
Security	Compliance Audit Artefacts	For Ever	SOC and other compliance
Security	Security Logs	1.5	APTs can take 18 months to detect

Business Area	Record Type	Maximum Retention Max (Yr)	Notes
Security	System access logs to record level	7	SOX
Security	System access audits	7	SOX
Security	Privacy Notices	7	GLBA for finance institutions
Security	Privacy and Security Training	6	HIPAA requires this