Data Protection and Backup Policy (ISP-10)

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 members of the IT department and data stewards.

Table of Contents

Introduction

Information Systems process and store data. Loss or corruption of this and system configuration data could severely impact the Universities day-to-day business. Data loss and corruption may occur because of a bad actor, through actions such as ransomware attacks or because of human error such as a data processor or administrator invertedly deleting a database table or a file share. As a result, it is important that data and configurations are backed up to a secure offsite location to ensure the availability and integrity of university data and operations. Additionally, those backups should be air gapped or immutable in nature to prevent threat actors from modifying or encrypting them to deny University access.

Objective

The Objective of this policy is to define the minimum measures that must be put in place to protect the data's integrity and availability.

Policy Statement

General

All systems that hold and store University data regardless of classification are to be protected by a backup system or service that at a minimum is required to perform a daily incremental, twice weekly full backup or equivalent. The minimum retention period for each of these are as follows:

Type	Low Priority Systems	High Priority Systems
Daily Incremental	30-days	30-days
Weekly Full	30-days	30-days

In addition to the above holistic backups, certain data sets such as financial and health care records are subject to legally required archiving.

All system configurations are to be captured systematically and subject to the same data protection measures.

All backups are to be encrypted to preserve the confidentiality of the data contained within them.

All backups are to include an offsite copy.

All backups are to be captured and either taken offline to implement an air gap or sent to immutable write once read many times media. This is to ensure bad actors cannot modify, delete, or encrypt the backup to deny access.

A test restore is to be performed bi-annually for all IT systems to ensure not only the integrity of the backups but that the restore process is operational.