Encryption Policy (ISP-07)

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 University IT and administrative staff.

Table of Contents

Introduction

University Information Systems are designed to protect the confidentiality and integrity of the information processed; be that the University's intellectual property and or personal information of our staff and students. The confidentiality of information is assured by encrypting data be it at rest or in transit; and Integrity is delivered by signing messages to ensure they are not tampered with. These two measures require the use of cryptographic modules and ciphers.

Objective

This policy's objective is to define when encryption and authentication are to be deployed and what standards and cipher sets are used.

Policy Statement

The University utilizes several software as a service (SaaS) platforms for enterprise functions as well as an array of infrastructure, networking, platform, and software services hosted on the campus. All these Information Systems are to adhere to the following:

1. All IT Systems are to perform user authentication prior to granting system access utilizing the University provisioned Hybrid OnPrem/Azure AD SSO solution.
2. All data is to be encrypted while in transit and at rest.
3. Only TLS v1.2 or newer is to be utilized.
4. To ensure standardization and deliver a robust security stance all University data is to be protected using the FIPS-140-2/3 compliant cipher suites defined below:

OpenSSL Cipher Suite Name	AT-TLS Cipher Suite Name
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
DHE-DSS-AES256-SHA	TLS DHE DSS WITH AES 256 CBC SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
EDH-DSS-DES-CBC3-SHA	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
DHE-DSS-AES128-SHA	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA

5. All cipher keys are to be stored in approved vaults, and those vaults are to be logically separated from the data the keys protect.
6. All cipher keys are to be protected with encryption while in transit and storage.
7. All systems that utilize encryption keys are to have a mechanism for key regeneration, rotation, and escrow.
8. At no time are symmetrical keys to be transmitted in the same channel or at the same time as the data that is being protected.
9. Cipher keys are to be used for only one purpose, i.e., encryption or authentication or signature, and discrete keys should be used for each communication route and or application component.
10. All systems must enable a method for revoking keys and replacing them. Material protected by

the revoked key must be re-encrypted with the current in force key.