Security Awareness and Training Policy (ISP-12)

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, students, and contractors who have access to University IT resources and services.

Table of Contents

Introduction

Security of data and IT systems is the responsibility of everyone. Systems are only as secure as the weakest component, which often is human. As such Cybersecurity and Awareness training is a valuable tool in improving user knowledge and therefore reducing overall cyber risk.

Objective

The Objective of this policy is to ensure all users understand the need for Cybersecurity Awareness and Education and are aware of their responsibilities to undertake said training.

Policy Statement

1. Upon being issued a University system account, all Users must complete Security Awareness Fundamentals Training consisting of a brief computer-based course. Information regarding how to access the training will be sent to users via University email.
2. Also, all users must periodically complete assigned computer-based cybersecurity training courses. The training courses are Internet based, and each takes 15 minutes to 1 hour to complete. Users can expect to spend between 1 and 2 hours per semester completing security awareness training.
3. Users will be given an appropriate amount of time to complete each training assignment. Users that do not complete assigned training within the specified time may have their user accounts revoked and will be required to complete all required training before the account is reinstated.
4. Users that are not employed by the University, including third-party vendors and contactors, may be exempted from the training requirements by providing evidence of the equivalent of at least 2 hours of cybersecurity related training within the last 6 months. Requests for exemption should be made to the CIO, CISO, QI, or IT Director’s office and must include evidence of prior training. An official determination will be made by the CIO, CISO, QI, or IT Director, and the requesting user will be notified.
5. The University utilizes tools and methods to monitor and assess IT security risk based on users’ network and computing behavior. Some users may be required to complete extra security and awareness training beyond the minimum training requirements set forth above.