POLICY STATEMENT 65.1
INFORMATION TECHNOLOGY SECURITY AWARENESS

POLICY DIGEST

Primary Monitoring Unit: Information Technology
Secondary Monitoring Unit: Chancellor
Initially Issued: May 20, 2020
Last Revised: None

I. INTRODUCTION

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all staff, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than Information Technology and network systems.

Lacking adequate information security awareness, faculty and staff are less likely to recognize or react appropriately to information security threats and incidents, and are more likely to place information assets at risk of compromise. In order to protect information assets, all workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

II. OBJECTIVE

This policy specifies the LSU Eunice internal information security awareness and training program to inform and assess all faculty and staff regarding their information security obligations.

III. SCOPE

This policy applies throughout the organization as part of the governance framework. It applies regardless of whether faculty or staff use computer systems and networks, since all employees are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This document also applies to third party employees working for the organization where applicable as determined by the LSU Eunice Office of Information Technology (OIT).

IV. AUDIENCE

In general, this document applies to all LSU Eunice employees and contractors with access to LSU Eunice systems, networks, campus information, nonpublic personal information, personally identifiable information, and/or user data.

V. RESPONSIBILITIES AND ACCOUNTABILITIES

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this program.

LSU Eunice OIT is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organization's and the organization's customer's information assets.

LSU Eunice OIT is responsible for developing and maintaining a comprehensive suite of information security policies, standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. OIT is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff's responsibilities.

All administrators are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All faculty and staff are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

VI. POLICY

All awareness training must fulfill the requirements for the security awareness program as listed below:

A. The information security awareness program should ensure that all employees achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, and regulations.

B. Additional training is appropriate for employees with specific obligations toward information security that are not satisfied by basic security awareness, for example IT/Network Operations personnel.

C. Security awareness and training activities should commence as soon as practicable after a hire joins the organization, generally through information security induction/orientation as part of the on boarding process. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

D. Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.

E. LSU Eunice will provide faculty and staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

VII. PROCEDURE

A. Information Security Awareness Training

The LSU Eunice OIT requires that each employee upon hire and at least annually thereafter successfully complete the courses that make up the Security Fundamentals Training program. These courses are currently:

1. Security Awareness Fundamentals Training Module
2. Phishing Fundamentals Training Module
3. FERPA Education

Certain employees may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Employees will be given a reasonable amount time to complete each course so as to not disrupt business operations.

B. Simulated Social Engineering Exercises

The LSU Eunice OIT will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), and physical assessments. The LSU Eunice OIT will conduct these tests at random throughout the year. The LSU Eunice OIT may conduct targeted exercises against specific departments or individuals based on a risk determination (see Appendix A.

C. Remedial Training Exercises

From time to time, LSU Eunice employees may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the LSU Eunice OIT as part of a risk-based assessment.

D. Compliance & Non-Compliance

Compliance with this document is mandatory for all employees, including contractors and executives. The LSU Eunice OIT will monitor compliance and non-compliance and report to the executive team the results of training and social engineering exercises. The penalties for non-compliance are described in Appendix B.

1. Non-Compliance Actions

Certain actions or non-actions by LSU Eunice employees may result in a non-compliance event (failure). A failure includes, but is not limited to:

a. Failure to complete required training within the time allotted
b. Failure of a social engineering exercise

Failure of a social engineering exercise includes, but is not limited to:

a. Clicking on a URL within a phishing test

b. Replying with any information to a phishing test

c. Opening an attachment that is part of a phishing test

d. Enabling macros that are within an attachment as part of a phishing test

e. Allowing exploit code to run as part of a phishing test

f. Entering any data within a landing page as part of a phishing test

g. Transmitting any information as part of a vishing (equivalent of phishing, but over telephone) test

h. Replying with any information to a smishing (equivalent of phishing, but through text) test

i. Failing to follow company policies in the course of a physical social engineering exercise

Certain social engineering exercises can result in multiple failures being counted in a single test. The maximum number of failure events per social engineering exercise is two.

The LSU Eunice OIT may also determine, on a case-by-case basis, that specific failures are a false positive and should be removed from that staff member's total failure count.

2. Compliance Actions

Certain actions or non-actions by LSU Eunice employees may result in a compliance event (Pass).

A pass includes, but is not limited to:

a. Successfully identifying a simulated social engineering exercises

b. Not having a failure during a social engineering exercise (Non-action)

c. Reporting real social engineering attacks to the IT department

E. Removing Failure Events through Passes

Each failure will result in a remedial training or coaching event as described in Appendix B of this document. Subsequent failures will result in escalation of training or coaching. De-escalation will occur when three consecutive passes have taken place.

VIII. DOCUMENT CHANGES AND FEEDBACK

This policy will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, update or changes to LSU Eunice requirements, technology, and the results or findings of any audit.

IX. SOURCES

Other documents that are relevant include the following:

LSUE Administrative Computing Policy https://www.lsue.edu/policy-statements/index.php
Employee Handbook Human Resources https://www.lsue.edu/faculty-staff/index.php

Appendix A – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of an LSU Eunice employee. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing.

- Employee is at an executive level (High value target)
- Employee possesses access to significant company confidential information
- Employee possesses access to significant company systems
- Employee has repeated violations

Appendix B – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance. Steps not listed here may be taken by the LSU Eunice OIT to reduce the risk that an individual may pose to LSU Eunice's computing system.

Security Training:

Failure to complete the security training program within the allocated timeframe will result in revocation of the employee's access into LSU Eunice's network and other systems. The employee's access will be restored once the training program has been completed.

Social Engineering Exercises:

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of the following training exercises/courses (or similar identified by OIT): • Spot the Phish Training Game • Phish Catcher Training Game
Second Failure	Mandatory completion of the following training exercises/courses (or similar identified by OIT): • Phishing Fundamentals • Phishing Andrew's Inbox
Third Failure	Mandatory completion of the following training exercises/courses (or similar identified by OIT): • 2020 Social Engineering Red Flags • 2020 Common Threats • 2019 Your Role: Internet Security and You
Fourth Failure	Face to face meeting with their manager
Fifth Failure	Face to face meeting with their manager and Human Resources
Sixth Failure	Face to face meeting with OIT Leadership and Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events (ex: restrictions around internet access)
Seventh Failure	Meeting with OIT Leadership, Chancellor, and Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events (ex: restrictions around internet access)