POLICY STATEMENT 120 STANDARD 3
SECURITY AWARENESS

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: October 17, 2022
Last Revised: none

I. PURPOSE

As an institution of higher education, Louisiana State University at Eunice ("University" or "LSU Eunice") is charged with maintaining systems and data for administrative and academic purposes. These assets are critical to the mission of the University, and the security of these systems and datasets must be managed with a formalized Information Security Program.

An element of protecting the University's information assets is ensuring that all LSU Eunice personnel understand their roles and responsibilities in protecting University systems, applications, data, etc. Additionally, it is critical to ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities, and of the applicable policies, standards, processes, and procedures related to the security of those systems. Both objectives can be addressed with effective security awareness measures.

The purpose of this standard is to describe the required components of security awareness as it relates to the Information Security Program at LSU Eunice.

II. DEFINITIONS

Asset. A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity's ability to continue business. Examples of assets including, but are not limited to,equipment, software, algorithms, and data.

Regulated data. Data controlled by federal, state, local, industry regulations, and/or contractual requirements. These datasets may have relevant data breach notification law as and contractual provisions which impose legal and technical restrictions on the appropriate use of the information.

University Employee. An individual who is employed by the University in any capacity, including independent contractors.

Users. All individuals that have access to University's assets through a University provided account.

Standard. Standards are defined actions and/or rules that provide support and direction for compliance with policies.

III. STANDARDS

A. 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 onboarding process. The awareness activities should continue on a rolling/continuous basis thereafter in order to maintain a reasonably consistent level of awareness.

B. 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.

C. 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.

D. The overall security awareness program would be led by LSU Eunice's Office of Information Technology (OIT).

E. The security awareness training shall be maintained and delivered via an enterprise security awareness training platform.

F. University must maintain appropriate records of course completion by all users.

G. University employees who fail to complete security awareness training may lose access to assets and face disciplinary actions as per the University policies.

IV. PROCEDURE

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

B. OIT requires that each employee complete the courses that make up the Security Fundamentals Training program. These courses currently include the following, but are subject to change:

1. Security Awareness Fundamentals

2. Phishing Fundamentals

3. FERPA Education

Employees will be given a reasonable amount time to complete each course so as to not

disrupt business operations.

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 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. 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 noncompliance 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.

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 OIT

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.

V. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	2/25/2022	Initial Draft	OIT

APPENDIX A

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

The following table outlines the penalty of non-compliance. Steps not listed here may be taken by the OIT to reduce the risk that an individual may pose to LSU Eunice's computing system. Any current exercises/courses identified are subject to change.

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 • Phish Catcher Training
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): • Social Engineering Red Flags • Common Threats • 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)