Information Security Awareness & User Training Program

Department: Campus Technology	**Date Created:** 3/24/2025
Owner: IT Department	**Date Last Revised:** 4/2/2025

Printed copies of this document are for reference only.

1. Plan Statement

The Information Security Awareness & User Training Program aims to establish best practices and guidelines for the IT Department's Information Security team to educate Lewis & Clark Community College employees, enhancing their preparedness for potential cyber threats.

1.1 Scope

The scope of this program applies to the designated information security personnel in the IT department.

1.3 Information Security Awareness & User Training

Information security awareness & user training is an essential program that aims to enhance the security posture of the college by providing all users with knowledge of potential cyber threats and the necessary information to accurately report them to IT. The training program consists of four elements:

- New hire training
- Annual team member training
- Simulated phishing exercises
- Simulated flash drive exercises

1.3.1 New Hire Training

All new team members are assigned to new hire training modules to educate them on cyber best practices, IT expectations, and how to report suspicious emails or activity. These training courses are refreshed periodically to ensure they are up to date with current IT department knowledge and cyber threats. This is to establish that the new employee has baseline knowledge of information security.

1.3.2 Annual Team Member Training

All current team members are assigned annual training modules to educate them on new cyber best practices, trends, IT expectations, and procedures. These courses are updated

yearly with current and foundational content to ensure employees have the latest information and are refreshed on relevant previous content.

1.3.3 Simulated Phishing Exercises

Information security personnel will conduct bi-annual phishing email simulations. These simulated emails will be sent to all Lewis & Clark Community College employees. The simulations are designed to accomplish several tasks:

- To enhance awareness of phishing emails across the college by exposing users with phishing emails that may normally be blocked by mail filters & rules.
- To provide sufficient practice in reporting emails to IT using the designated reporting channels.
- The opportunity to generate data on the effectiveness of the information security awareness campaigns/ trainings.

The use of simulated phishing emails aims to increase the effectiveness of the college's security posture and allows for IT to continue to improve it from the data it provides.

1.3.4 Simulated Flash Drive Exercises

Information security encompasses both digital and physical storage devices. Due to the frequent use of flash drives and external storage at the college, the IT department conducts bi-annual flash drive exercises.

These exercises test employees' ability to report suspicious flash drives placed across campus, thereby evaluating the effectiveness of the security awareness campaign and providing opportunities for employees to report suspicious media.

1.4 Program Effectiveness

The awareness & user training program's effectiveness is measured by several key performance indicators (KPIs):

- A proficiency assessment provided at the end of each training campaign
- The results of the simulated phishing and flash drive drop campaigns
- The average scores of quizzes and assessments throughout the training campaigns.

These three factors provide evidence of where team members (employees) are and are not proficient. The data from these three KPIs provide insight where the future of the program will focus to ensure that team members are adequately provided knowledge and practice to strengthen the college's overall cyber-literacy.

1.5 Designated Personnel Training

All information security personnel must undergo required continuous training to keep up with information security trends to adequately understand what tactics and content team members will require to successfully be able to detect suspicious activity. All IT employees have access to an online training source for a wide variety of IT knowledge and must

regularly educate themselves on current information security content or refresh themselves on previously learned content.

Information security personnel will periodically attend cybersecurity conferences to network and learn with industry peers and vendors to learn about the latest trends and tactics to broaden their knowledge of the industry.

1.6 Enforcement

If this program is failed to be carried out by the IT department, an action plan must be created and demonstrated to resolve any issues with the program. All information regarding the program is to be reported to the Chief Data & Technology Office to be reported to the board in the information security plan's annual report.

1.7 Program Review

This program shall be reviewed and updated periodically by the IT department to ensure its effectiveness and compliance with relevant laws, regulations, and industry standards.

1.8 Revision history

Below is the recorded history of the program. This must be updated each time the program undergoes changes.

Date	Change Description	Author - Position	Approved By - Position
3-24-2025	Documentation creation	McLaughlin – Information Security Analyst	-
3-26-2025	Documentation revisions to add the simulated phishing and flash drive tests. To be sent to the CDTO for review	McLaughlin – Information Security Analyst	-
4-1-2025	Removed the placeholder section and fixed the section numbering. Sent to CDTO for review	McLaughlin – Information Security Analyst	-
4-2-2025	CDTO accepted changes. Prepared for approval	McLaughlin – Information Security Analyst	Ron Wall

-----END OF DOCUMENT-----