Procedure: Security Awareness Program Plan	
Issue Date: 5/1/2022	**Revision Date:**
Revision Number: 1.1	**NIST Control: AT**
Owner: Director of Information Technology	

Contents

THE Wesleyan Way KENTUCKY WESLEYAN COLLEGE	*AWARENESS PROGRAM PLAN*
Effective Date 1/1/2023	Version 1.0

1. Overview

1.1 Security Awareness Program

This program described herein will provide Kentucky Wesleyan College with a comprehensive and measurable awareness program. Based on the globally recognized NIST SP800-16 and NIST SP800-50 standard for Information Technology Security Training and industry recommended practices, the program will help to ensure that Kentucky Wesleyan College is proactively identifying and addressing the security risks presented by people.

2. Scope

This program is designed to address the security awareness and training needs of all Kentucky Wesleyan College departments, divisions, locations, roles, and responsibilities. The program will assist Kentucky Wesleyan College with designing, planning, and implementing a security awareness and training program. The intended audiences include, but are not limited to employees, faculty, and vendor/third-parties. An awareness program should be aimed at all levels of the organization which also includes senior management.

A successful security awareness and training program identifies and explains the proper behaviors when handling different devices and information. Success also relies on the security awareness and training becoming part of the organization's culture. The program will communicate the guidelines, policies, and best practices that need to be followed.

3. Program Considerations

Kentucky Wesleyan College has taken then following areas into consideration when designing and implementing a security awareness program:

- The individual or team that will be responsible for overseeing the implementation and maintenance of the program;

- Timeframe for completion of the security training for new hires;
- A need for training due to a compliance or regulatory requirement to meet;
- Frequency of training and testing (e.g. annually, quarterly, monthly);
- The type of training content and methods by which training will be delivered;
- Groups and individuals to include in the training;
- Time constraints and availability;
- Senior leadership buy-in to carry out training and testing; and
- How non-compliance will be handled and enforced.

This program will be delivered over the course of one year and may include, but is not limited to:

- Instructor-led training;
- Computer-based training using quizzes, tests, or videos; and
- Social engineering.

While this program describes the collective awareness efforts across all Kentucky Wesleyan College departments, it is anticipated that specific role-based training and awareness may be required for each audience.

4. Program Roles and Responsibilities

The Director of Information Technology is:

- Responsible for implementing, developing, and maintaining the overall Awareness Program for Kentucky Wesleyan College.
- Responsible for coordinating with business departments and units to ensure participation and completion of training.
- Responsible for tracking attendance to training sessions in personnel files and obtaining and filing any attestations or post-training quizzes or tests.
- Responsible for scheduling and conducting on-site training, on-site table events, computer-based training and/or performing any social engineering testing.

5. Awareness and Training Strategy

At a minimum, employees will be required to take general security awareness training at least annually. All new hires of the organization will have 30 days to complete their security awareness training.

1.2 Information Security and Cybersecurity Best Practices

This training is offered via computer-based education based on the NIST SP800-16 (See References) standard and recommended practices. This training typically takes 15-45 minutes to complete. At a minimum, the training will cover:

- Current Threats and Common Attacks
- Data Protection
- Security Policies and Procedures
- Privacy
- Recommended Security Best Practices for:
    - Passwords
    - E-Mail
    - Web Browsing
    - Mobile Devices
    - Social Media
    - Wireless Networks
    - Antivirus
    - Social Engineering
        - Phishing
        - Vishing
    - Physical Security
- Identifying and Responding to Incidents

1.3 Additional Training Areas

All additional Awareness trainings are computer-based education based on a variety of relevant regulations, laws and commercial requirements targeting groups of people that

have specialized roles, privileges, or risks. Additional training topics may include, but are not limited to:

- ***Health Insurance Portability and Accountability Act (HIPAA)***
- ***Family Education Rights and Privacy Act (FERPA)***
- ***Data Classification Handling Procedure***s
- ***Cybersecurity for IT***
- ***Cybersecurity for Senior Management***
- ***Cybersecurity for Travelers***
- ***Gramm-Leach-Bliley Act***
- ***EU General Data Protection Regulation***

1.4 Training Metrics

The security awareness program should capture metrics that measures the overall human risk and behaviors. The metrics should ensure that the organization's awareness program is compliant with regulatory requirements and if human behavior is changing. Additional metrics that can be captured, but not limited to are:

- Number of employees that attended last training;
- Number of users reporting phishing attacks;
- Number of users falling victim to phishing attacks.
- Number of users who fail sanctioned phishing tests.

Additional assessments may be necessary to capture the overall effectiveness of the security awareness program.

1.5 Training Records

Training records will be kept in accordance with the college's security risk assessment guidance. Employee training records will be available to Human Resources on demand.

6. Testing/Assessments

1.6 Testing – Social Engineering

Social Engineering – In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Social engineering tests should be conducted on a regular basis to continuously measure the susceptibility of employees to common attacks. Tests and assessments may be delivered in the following formats:

- Phishing – Sending e-mails with links, attachments and other requests
- Physical – Physical impersonation or intrusion to access control areas or physical walk-through of office space to detect security deficiencies or violations

Results of social engineering tests will be incorporated into the overall program and tracked. The Director of Information Technology will be responsible for any further follow-up and training.

7. Non-Compliance

The Director of Information Technology will work in conjunction with Human Resources to ensure all employees complete their required training. In the event that an employee fails to complete their security training the organization will take the following actions:

- Employees will be notified of their non-compliance and their time to complete the training will be extended by 2 weeks.
- Failure to complete training after the 2-week extension, the employee's manager or supervisor will be notified.
- Failure to complete training after additional notification may lead to loss of access to the college's systems and/or additional sanctions as deemed appropriate by Human Resources.

8. Timeline

1.7 Training Plan

Title	Audience	Number of Sessions	Frequency	Complete By:
Security Awareness Proficiency Assessment	All Faculty, Staff	1	Annually	Information Security Team
Security Awareness Training	All Faculty, Staff	1	Ongoing	Information Security Team
Incident Response Tabletop	Information Technology Team	1	Annually	Information Security Team

1.8 Testing Plan

Type	Format	Number of Tests	Frequency	Complete By:
Social Engineering	Phishing	Bi-weekly	Ongoing	Information Technology Team
	Physical observation checks	Continuously	Ongoing	Information Technology Team

9. References

- NIST SP 800-16 Information Technology Security Training
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

10. Revisions

Version	Date	Responsible	Revisions
1.0	5/1/2022	GreyCastle Security	Initial Draft
1.1		KWC	Review, Finalize, Approve, Publish