ALVIN COMMUNITY COLLEGE	ADMINISTRATIVE PROCEDURE MANUAL	
Section Title: Cyber Safety Awareness Training and Testing Program	Number: cr-04	Page: 1 of 6
BASED ON BOARD OF REGENTS POLICY		
Policy Title: TECHNOLOGY RESOURCES	Policy Number: CR	
Local	Date Adopted by ELT: 12/12/17	

Purpose

The purpose of this procedure is to provide information on the colleges security awareness training and testing program.

1. Background

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 IT and network systems.

Lacking adequate information security awareness, staff is 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.

2. Scope

This Program applies throughout the organization as part of the corporate governance framework. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This Program also applies to third party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

3. Program

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

a. The cyber safety awareness program must ensure that all staff 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, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

b. Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.

c. Security awareness and training activities must commence as soon as practicable after staff joins the organization, generally through attending 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 training materials and exercises must 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. ACC will provide 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.

f. Alvin Community College's Information Technology Services (ITS) department requires that each employee upon hire and at least annually thereafter successfully complete at minimum, a basic cyber safety awareness training course. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually, as referenced in Appendix B – Methods for Determining Staff Risk Ratings. Staff will be given a reasonable amount time to complete each course so as to not disrupt business operations.

g. ITS will conduct periodic simulated social engineering exercises including but not

limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. ACC ITS will conduct these tests at random throughout the year with no set schedule or frequency. ACC ITS may conduct targeted exercises against specific departments or individuals based on a risk determination.

h. From time to time ACC staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of ACC ITS as part of a risk-based assessment.

4. **Compliance**

Compliance with this Program is mandatory for all staff, including contractors and executives. Alvin Community College Information Technology Services will monitor compliance and non-compliance with this Program and report to the executive team the results of training and social engineering exercises. The penalties for non-compliance are described in Appendix A – Schedule of Failure Penalties.

a. **Compliance Actions:** Certain actions or non-actions by ACC personnel may result in a compliance event (Pass).
A pass includes but is not limited to:
- Successfully identifying a simulated social engineering exercises
- Not having a failure during a social engineering exercise (Non-action)
- Reporting real social engineering attacks to the IS department

b. **Non-Compliance Actions:** Certain actions or non-actions by ACC personnel may result in a non-compliance event (Failure).

A Failure includes but is not limited to:
- Failure to complete required training within the time allotted
- Failure of a social engineering exercise

Failure of a social engineering exercise includes but is not limited to:
- Clicking on a URL within a phishing test
- Replying with any information to a phishing test
- Opening an attachment that is part of a phishing test
- Enabling macros that are within an attachment as part of a phishing test
- Allowing exploit code to run as part of a phishing test
- Entering any data within a landing page as part of a phishing test
- Transmitting any information as part of a vishing test
- Replying with any information to a smishing test
- Plugging in a USB stick or removable drive as part of a social engineering exercise
- Failing to follow ACC 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.

ACC ITS 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.

c. Removing Failure Events through Passes

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

5. Responsibilities and Accountabilities

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

a. The Director, Information Technology is accountable for running an effective cyber safety awareness and training program that informs and motivates workers to help protect the organization's and the organization's customer's information assets.

b. The Network Security Administrator is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other institutional functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff's responsibilities identified in applicable policies, laws, regulations, contracts, etc.

c. All supervisors 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.

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

Appendix A – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance with this Program. Steps not listed here may be taken by the ACC ITS team to reduce the risk that an individual may pose to the College.

Failure Count Level	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of Cyber-Safety awareness course I.
Second Failure	Mandatory completion of Cyber-Safety awareness course II and face to face meeting with their manager.
Third Failure	Mandatory completion of Cyber-Safety awareness course III and face to face meeting with their manager and Executive Director of Human Resources.
Fourth Failure	Face to face meeting with their manager, Executive Director of Human Resources, Director of Information Technology, and Executive Leadership Team member.
Fifth Failure	Face to face meeting with their manager, Executive Director of Human Resources, Directory of Information Technology, Executive Leadership Team member, and College President. - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events (including restriction or removal of access to networked resources)
Sixth Failure	Formal review of employment with Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events (including restriction or removal of access to networked resources)
Seventh and Subsequent Failures	Potential for Termination of Employment or Employment Contract

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of an Alvin Community College 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.

- Staff member email resides within a recent Email Exposure Check report
- Staff member is an executive or VP (High value target)
- Staff member possesses access to significant ACC confidential information
- Staff member is using a Windows or Apple-based operating system
- Staff member uses their mobile phone for conducting work-related business
- Staff member possesses access to significant ACC systems
- Staff member personal information can be found publicly on the internet
- Staff member maintains a weak password
- Staff member has repeated Security Awareness Program violations