Rogers State University Security Awareness Training and Testing

Document Owner	Title
Brian Reeves	Director of Information Technology

Document History

Rev #	Name	Date	Description	Signature
1.0	Brian Reeves	7-1-2020	Initial draft	Brian
1.1	Quince Fennell	20200723	Review	Q
1.2	Brian Reeves	8/10/2020	Adjusted training requirements	Brian
1.3	Brian Reeves	8/25/2020	Fixed minor type in the table of contents	Brian

Date: 8/25/2020

approved 8-24-2000

Table of Contents

1. 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 IT and network systems.

Lacking adequate information security awareness, staff is less likely to recognize or react appropriately to information security threats, 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.

1.1 Objective

This policy specifies the Rogers State University (RSU) internal information security awareness and training program to inform and assess all staff regarding their information security obligations.

1.2 Scope

This policy applies throughout the organization. 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 policy 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.

1.3 Audience

This policy applies to all RSU employees and contractors with access to RSU systems, networks, company information, nonpublic personal information, personally identifiable information, and/or customer data.

1.4 Document Changes and Feedback

This policy will be reviewed at least annually to reflect, among other things, changes to applicable law, update or changes to RSU requirements, technology, and the results or findings of any audit.

2. Policy Requirements

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

- The information security awareness program should 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.
- Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness.
- Security awareness and training activities should commence as soon as practicable after staff joins the organization. The awareness activities should be conducted on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.
- 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.

- RSU will provide staff and faculty 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.

2.1 RSU Information Security Awareness Training

RSU requires that each employee must successfully complete Security Awareness Fundamentals. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will be given a reasonable amount time to complete each course to not disrupt business operations.

2.2 Simulated Social Engineering Exercises

RSU will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. RSU will conduct these tests at random throughout the year with no set schedule or frequency. RSU may conduct targeted exercises towards specific departments or individuals based on a risk determination.

2.3 Remedial Training Exercises

From time to time RSU staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the Academic Computing Services (ACS) as part of a risk-based assessment.

3. Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all faculty, staff and adjuncts. ACS will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

The penalties for non-compliance are described in Appendix A of this policy.

3.1 Non-Compliance Actions

Certain actions or non-actions by RSU 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 company policies during 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.

ACS 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.

3.2 Compliance Actions

Certain actions or non-actions by RSU personnel may result in a compliance event (Pass).

A Pass includes but is not limited to:

- Successfully identifying a simulated social engineering exercise
- Not having a Failure during a social engineering exercise (Non-action)
- Reporting real social engineering attacks to the IS department

3.3 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 three consecutive Passes have taken place.

4. Responsibilities and Accountabilities

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

Director of Information Technology – Is responsible for maintaining and reviewing this policy. The Director of Information Technology will provide compliance reports to the President's Cabinet.

Cyber-Security Specialist 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.

All Managers 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 Staff are personally accountable for completing the security 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 policy.

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of Security Awareness Fundamentals
Second Failure	Mandatory completion of Security Awareness Fundamentals
Third Failure and Additional Failures	Mandatory completion of Security Awareness Fundamentals and Face to face meeting with their Department Head. A notice will also be sent to HR for the employee's file.

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of a RSU 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 company confidential information
- Staff member has access to the VPN
- 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 company systems
- Staff member personal information can be found publicly on the internet
- Staff member maintains a weak password
- Staff member has repeated company policy violations