Cyber Security Awareness Training and Testing

Document Owner	Title
Jodi Nestich	Information Technology Director

Document History

Rev #	Name	Date	Description	Signature
1.0	Jodi Nestich	1/12/2023	Initial draft	Electronically signed
1.1	Matthew Newton	4/13/2023	Initial release	Owner signature
1.2	Jodi Nestich	1/31/2024	Review	Electronically signed

Version: 1.2
Date: January 12, 2023
Adopted: April 13, 2023
M-55-23
Reviewed: January 31, 2024

SSecurity Awareness Training

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 and incidents thus 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 CASS COUNTY 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 as part of the organizational 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 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

In general, this policy applies to all CASS COUNTY employees and contractors with access to CASS COUNTY systems, networks, Cass County information, nonpublic personal information, personally identifiable information, and/or data.

1.4 Document Changes and Feedback

This policy will be updated and re-issued as needed to reflect, among other things, changes to applicable law, update or changes to CASS COUNTY 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, for example the requirements set forth by the Criminal Justice Information Services. 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.

- Security awareness and training activities should 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 be on a continuous/rolling basis thereafter 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 Elected Officials and Department Heads with broader responsibilities to the organization and their staff.
- Cass County 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.

2.1 CASS COUNTY Information Security Awareness Training

CASS COUNTY requires that each employee upon hire and at least quarterly thereafter successfully complete security awareness training. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire. Staff will be given a reasonable amount time to complete each course so as to not disrupt business operations.

2.2 Simulated Social Engineering Exercises

The CASS COUNTY IT DEPARTMENT will conduct periodic simulated social engineering exercises including but not limited to phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The CASS COUNTY IT DEPARTMENT will conduct these tests at random throughout the year with no set schedule or frequency.

2.3 Remedial Training Exercises

From time-to-time Cass County staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the Cass County IT Department as part of a risk-based assessment.

3. Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all employees, including contractors and executives. Monitoring will be conducted for compliance and non-compliance with this policy. The results of training and social engineering exercises will be reported to Elected Officials and Department Heads.

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

3.1 Non-Compliance Actions

Certain actions or non-actions by CASS COUNTY 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 Cass County 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.

The Cass County IT Department 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 CASS COUNTY 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 IT 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.

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

Information Security Management 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 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.

Elected Officials agree that their staff and other workers under 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. Steps not listed here may be taken by the CASS COUNTY IS team to reduce the risk that an individual may pose to the Cass County.

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of training course
Second Failure	Mandatory completion of training course
Third Failure	Mandatory completion of training course
Fourth Failure	Face to face meeting with their Elected Official or Immediate Supervisor
Fifth Failure	Face to face meeting with their Elected Official or Immediate Supervisor and IT Director to develop personalized training for security concepts

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of a CASS COUNTY staff member. 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 Elected Official, Administrator or Department Head (High value target)
- Staff member possesses access to significant Cass County 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 Cass County systems
- Staff member personal information can be found publicly on the internet
- Staff member maintains a weak password
- Staff member has repeated Cass County policy violations

Appendix C – Glossary of Terms if Applicable