

# TOWN OF ELLINGTON

## Policies & Procedures

### Security Awareness Training and Testing Policy

#### 1.0. 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, and anyone who has been issued a Town email account, 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, users are 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 email account users must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

#### 1.1 Objective

This policy specifies the Town of Ellington's internal information security awareness and training program to inform and assess all staff, and anyone who has been issued a Town email account, regarding their information security obligations.

#### 1.2 Scope

This policy applies to staff and anyone who has been issued a Town email account.

#### 1.3 Audience

In general, this policy applies to all Town of Ellington employees and anyone who has been issued a Town email account, in addition to contractors with access to Town of Ellington systems, networks, Town information, and/or customer data.

#### 1.4 Document Changes and Feedback

This policy will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, update or changes to Town of Ellington requirements, technology, and the results or findings of any audit.

#### 1.5 Referenced Documents

Documents that are relevant to this policy include the following: Personnel Rules & Regulations.

## **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 users achieve and maintain at least a basic level of understanding of information security matters.
- Additional training is appropriate for staff, and anyone who has been issued a Town email account, 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 a Town email account has been issued. The awareness activities should continue 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.

### **2.1 Town of Ellington Information Security Awareness Training**

The Town of Ellington Information Security Awareness Training requires that anyone who has been issued a Town email account successfully complete annual KnowBe4 Security Awareness Training. Certain users may be required to complete additional training modules depending on their specific job or responsibility requirements and at least annually. Users 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 Town of Ellington IT Technician will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (text), USB (flash drive) testing, and physical assessments. These tests will be conducted at random throughout the year with no set schedule or frequency. The Town IT Technician may conduct targeted exercises against specific departments or individuals based on a risk determination.

### **2.3 Remedial Training Exercises**

From time to time Town of Ellington email account users may be required to complete remedial training courses or may be required to participate in remedial training exercises with the Town IT Technician as part of a risk-based assessment.

## **3. Compliance & Non-Compliance with Policy**

Compliance with this policy is mandatory for all staff and anyone who has been issued a Town email account. The Town of Ellington IT Technician will monitor compliance and non-compliance with this policy and report to Human Resources 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 Town of Ellington 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 phishing 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 Town 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 Town of Ellington IT Technician may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that user's total Failure count.

### **3.2 Compliance Actions**

Certain actions or non-actions by Town of Ellington 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 Town of Ellington IT Technician.

### **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 two 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 Town of Ellington IT Technician and the Town of Ellington Risk Control Manager are accountable for running an effective information security awareness and training program that informs and motivates the Town email account user to help protect the Town and the Town's information assets. The Town of Ellington IT Technician and the Town of Ellington Risk Control Manager are also 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.

All Department Heads 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 and anyone who has been issued a Town email account are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

Board of Selectmen Approved: 12/10/2018

### 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 Town of Ellington to reduce the risk that an individual may pose to the Town.

<b>Failure Count</b>	<b>Resulting Level of Remediation Action</b>
First Failure	Mandatory completion of Remedial Security Awareness Training
Second Failure	Mandatory completion of Remedial Security Awareness Training and meeting with Department Head and/or Risk Control Manager.
Third Failure	The Town may impose appropriate disciplinary action in the event of an employee's failure to comply with this policy, in accordance with the Town's Personnel Rules and Regulations. For non-employee users, escalation of training or coaching will be implemented by the Risk Control Manager.

**SECURITY AWARENESS TRAINING & TESTING POLICY**

**ACKNOWLEDGEMENT FORM**

I have read and understand the Town of Ellington Security Awareness Training & Testing Policy and agree to follow all policies and procedures that are set forth therein. Furthermore, I understand this document can be amended at any time.

Name: \_\_\_\_\_  
(Please print)

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Please return completed form to the Human Resources Office.