City of Pitt Meadows
THE Natural PLACE

ADMINISTRATIVE POLICY A047

04 - Information Systems & Services

Security Awareness Training and Testing

Effective Date: February 17, 2022
Last Revised:
CAO Signature:

Policy Statement

1. Technical security controls are a vital part of the City's 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.

2. 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.

Purpose

3. This policy specifies the City of Pitt Meadows internal information security awareness and training program to inform and assess all staff regarding their information security obligations.

Scope

4. 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.

Exclusions

5. The Chief Administrative Officer may grant standing or single instance exemptions to this policy where a valid business reason exists.

Definitions

6. In this policy,

   (a) *Social Engineering* means the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

   (b) *Phishing* means the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

   (c) *Smishing* means the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

   (d) *Vishing* means the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Roles and Responsibilities

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

   (a) The Information Technology Manager is accountable for running an ongoing 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.

   (b) Information Technology 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 corporate 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 **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.

(d) All **Staff** are accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

Prohibitions

8. None identified.

Procedures and Guidelines

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

(a) 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.

(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 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 continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

(d) 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.

(e) The City 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.

10. City Information Security Awareness Training

(a) The City Information Technology (IT) department requires that each employee upon hire and periodically thereafter successfully complete courses as deemed fit and appropriate by the Manager of IT. 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 of time to complete each course so as to not disrupt business operations.

11. Simulated Social Engineering Exercises.

(a) The City's 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 primary objectives of simulation exercises are as follows:

(i) To be used as a cyber-security awareness educational tool;

(ii) To assess the City's current level of cyber security awareness;

(iii) To measure the effectiveness of the City's Cyber Security Awareness and Training Program over time and compare to benchmark data and industry norms ;

(iv) The City's IT department will conduct simulation exercises at random throughout the year with no set schedule or frequency. The City's IT department may conduct targeted exercises against specific departments or individuals based on a risk determination.

12. Determining Staff Risk

(a) The following are factors that determine a risk rating of a City 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.

(i) Staff member email resides within a recent Email Exposure Check report;

(ii) Staff member is an executive or (High value target);

(iii) Staff member possesses access to significant confidential information;

(iv) Staff member is using a Windows or Apple-based operating system;

(v) Staff member uses their mobile phone for conducting work-related business;

(vi) Staff member possesses access to significant City systems;

(vii) Staff member personal information can be found publicly on the internet;

(viii) Staff member maintains a weak password;

(ix) Staff member has repeated City policy violations;

(x) Staff member repeatedly fails simulation exercises.

(b) IT will maintain a unique Risk Rating for each user. Risk ratings may be used to identify remedial training opportunities for individual staff or groups. Collectively staff risk ratings will be used to calculate the Risk Score for the entire organization. The City's risk score will be used to evaluate the effectiveness of the City's security awareness program over time and against industry peers.

13. Remedial Training Exercises

(a) From time to time City staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the City's IT department as part of a risk-based assessment.

14. Compliance & Non-Compliance with Policy

(a) Compliance with this policy is mandatory for all staff. The City IT department will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

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

(i) A Failure includes but is not limited to:

- Failure to complete required training within the time allotted;
- Failure of a social engineering exercise.

(ii) 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 City policies in the course of a physical social engineering exercise.

(c) Compliance Actions. Certain actions or non-actions by City personnel may result in a compliance event (Pass).

(i) 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

Related Policies

15. Other related policies include:

(a) A002 – Mobile Client Computing Technology

(b) A009 – Acceptable Use of Information Technology