Town of
SLAVE LAKE

TOWN OF SLAVE LAKE INFORMATION TECHNOLOGY POLICY			
Directorate	Corporate Services		
Department:	Information Technology	Policy No:	CRS.IT-23.1000
Policy Title:	Security Awareness Training and Testing	Issue Date:	
Issued to:	All Employees	Policy Type:	New

Policy Statement

1. Our policy recognizes that while technical security controls are essential, they alone cannot fully secure all information assets. The active participation and awareness of all staff members are crucial in achieving effective information security. This is particularly evident in the face of social engineering attacks and other exploits that specifically target vulnerable individuals rather than IT systems.
2. Insufficient information security awareness among staff increases the risk of compromised information assets and ineffective response to security threats and incidents. To mitigate this risk, it is imperative that all employees are well-informed about current information security issues and motivated to fulfill their information security obligations.
3. By promoting comprehensive information security awareness, we aim to enhance the protection of our information assets. This involves ongoing training and education initiatives to ensure that staff members are equipped to recognize and respond appropriately to information security threats. Through the combined efforts of technical security controls and staff awareness, we strive to create a secure information environment that safeguards the confidentiality, integrity, and availability of our organization's assets.

Purpose:

4. This policy aims to provide clear guidelines for security awareness training and testing within the Town of Slave Lake. Its purpose is to educate employees about potential security risks, enhance their knowledge of security best practices, and foster a proactive approach to maintaining a secure environment. By establishing these guidelines, we seek to mitigate the

5. likelihood of security incidents and promote a culture of vigilance and responsibility among our staff.

Scope:

6. This policy applies to all employees, contractors, and third-party personnel who have access to the systems, networks, or sensitive information of the Town of Slave Lake. It is applicable to individuals across all departments and levels within the organization, ensuring a comprehensive approach to maintaining security awareness and protecting valuable assets.

Exemptions

7. The Chief Administrative Officer holds the authority to grant standing or single instance exemptions to this policy based on valid business reasons. Such exemptions may be considered in exceptional cases to accommodate specific circumstances while ensuring the overall security objectives of the Town of Slave Lake are upheld.

Definitions

7. In this policy,

(a) Social Engineering: Refers to the deceptive tactics employed to manipulate individuals into disclosing confidential or personal information, which can be exploited for fraudulent purposes.

(b) Phishing: Denotes the fraudulent practice of sending deceptive emails that appear to originate from reputable companies, with the intention of tricking individuals into divulging personal information, such as passwords and credit card numbers.

(c) Smishing: Describes the fraudulent practice of sending text messages that falsely claim to be from reputable companies, with the aim of persuading individuals to disclose personal information, such as passwords or credit card numbers.

(d) Vishing: Signifies the fraudulent practice of making phone calls or leaving voice messages that falsely represent reputable companies, with the objective of coercing individuals into revealing sensitive information, such as bank details and credit card numbers.

Roles and Responsibilities:

8. Outlined below are the key responsibilities and accountabilities associated with managing and complying with this policy program:

(b) Corporate Services Director:

The Corporate Services directorate holds the responsibility for developing and upholding a comprehensive set of information security policies, including this policy. They are also tasked with establishing standards, procedures, and guidelines that are mandated or endorsed by management when applicable. Working in collaboration with other corporate functions, they are responsible for conducting suitable awareness, training, and educational activities to raise awareness and facilitate understanding of staff members' responsibilities as outlined in relevant policies, laws, regulations, contracts, etc.

(a) The Information Technology Manager:

The Information Technology Manager bears the accountability for implementing and maintaining an effective information security awareness and training program. This program aims to inform and motivate employees to protect the organization's and its customers' information assets.

(c) All Managers and Directors:

All managers and directors are responsible for ensuring that their staff and other workers under their supervision actively participate in information security awareness, training, and educational activities as deemed appropriate and necessary.

(d) All Staff:

All staff members are accountable for completing security awareness training activities and adhering to applicable policies, laws, and regulations always. They

are expected to actively engage in maintaining information security and fulfilling their responsibilities to protect organizational information assets.

By clearly defining these roles and responsibilities, we aim to foster a culture of shared accountability and ensure that all stakeholders are actively involved in promoting and upholding effective information security practices within the organization.

Prohibitions

9. None identified.

Procedures and Guidelines:

10. The following procedures and guidelines outline the requirements and expectations for the security awareness training and testing program within the Town of Slave Lake:

(a) Information Security Awareness Program:

The information security awareness program aims to ensure that all staff members acquire and maintain a fundamental level of understanding regarding information security matters. This includes their obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally accepted standards of ethics and behavior.

(b) Additional Training:

Staff members with specific information security responsibilities beyond the basic security awareness level, such as Information Risk and Security Management, Security Administration, Site Security, and IT/Network Operations personnel, should receive additional training. These training requirements should be identified in departmental or personal training plans and be adequately funded. Consideration should be given to relevant prior experience, training, professional qualifications, and anticipated job requirements.

(c) Commencement of Awareness Activities:

Security awareness and training activities should commence promptly after staff members join the organization, typically through information security induction or orientation during the onboarding process. Continuous and ongoing awareness activities should be conducted to maintain a reasonably consistent level of awareness among staff members.

(d) Tailoring of Materials and Exercises:

Security awareness training materials and exercises should be customized to suit the intended audiences, considering factors such as styles, formats, complexity, technical content, and other relevant aspects.

(e) Provision of Information:

The Town of Slave Lake will provide staff members with information about the location of security awareness training materials. They will also have access to security policies, standards, and guidance relating to various information security matters.

11.Town of Slave Lake Information Security Awareness Training:

(a). The Town's Information Technology (IT) department mandates that all employees successfully complete designated courses upon hire and periodically thereafter, as determined by the IT Manager. Additional training modules may be required based on specific job requirements. Adequate time will be provided to complete each course without disrupting business operations.

12.Simulated Social Engineering Exercises:

(a). The Town's IT department will conduct periodic simulated social engineering exercises, including phishing (email), vishing (voice), smishing (SMS), USB testing, and physical assessments. These exercises serve as educational tools, assess the level of cyber security awareness within the organization, measure the effectiveness of the Cyber Security Awareness and Training Program over time, and identify areas for improvement. The exercises may be conducted randomly throughout the year, with targeted exercises based on risk assessments.

13.Determining Staff Risk:

(a). Factors such as email exposure, executive roles, access to confidential information, operating system usage, mobile phone usage for work-related tasks, system access, public availability of personal information, weak passwords, policy violations, and performance in simulation exercises are considered when determining the risk rating of Town staff members. Risk ratings help identify remedial training opportunities and calculate the overall risk score to evaluate the effectiveness of the security awareness program.

14.Remedial Training Exercises:

(a). Town staff may be required to participate in remedial training courses or exercises as part of a risk-based assessment conducted by the IT department.

15.Compliance & Non-Compliance with Policy:

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

(b) Non-Compliance Actions: Failure to adhere to this policy may result in a non-compliance event (Failure). Examples of Failure include, but are not limited to:

(i) Failure to complete required training within the specified timeframe.

(ii) Failure in a social engineering exercise, which includes actions such as:

- Clicking on a URL within a phishing test.
- Providing any information in response to a phishing test.
- Transmitting any information in response to a vishing test.
- Providing any information in response to a smishing test.
- Connecting a USB stick or removable drive as part of a social engineering exercise.
- Failing to comply with Town policies during a physical-social engineering exercise.
- Opening an attachment that is part of a phishing test.
- Enabling macros within an attachment as part of a phishing test.
- Allowing exploit code to run as part of a phishing test.

- Entering data on a landing page as part of a phishing test.

(c) Compliance Actions: Certain actions or non-actions by Town personnel may result in a compliance event (Pass). Examples of a Pass include, but are not limited to:

- Successfully identifying simulated social engineering exercises.
- Demonstrating a non-action Failure during a social engineering exercise.
- Reporting real social engineering attacks to the IS department.

16.Related Policies:

This policy should be read in conjunction with the following related policies:

CRS.IT-23.1001 – Mobile Client Computing Technology

CRS.IT-23.1002 – Acceptable Use of Information Technology

These related policies provide additional guidance and requirements that support the objectives and implementation of this Security Awareness Training and Testing Policy.

Policy Review:

This policy will be reviewed periodically to ensure its effectiveness and relevance to the evolving security landscape. Updates or revisions to the policy will be communicated to all employees.

ISSUED BY	APPROVED BY:	DATE:
1. Chief Administrative Officer		Sept. 15/23