IT Security Incident Management

Policy No.: CS-IT-9	**Council Resolution No.:** 394/2020
Department: Information Technology	**Authority:** Council
Effective Date: September 28, 2020	**Revision Date:**
Review Date: September 2023	**Repealed Date:**
Supersedes: N/A	
Related Procedure No.: CS-IT-9	
Related Procedure Name: IT Security Incident Management	

Purpose

This Policy serves to ensure proper recognition, management, and communication of security events and weaknesses through a formal process.

The quality and integrity of the Town's incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and respond to these incidents. Without an incident response capability, the potential exists that in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected sooner.

Policy Statement

1) This Security Incident Management Policy applies to all business processes and data, information systems and components, personnel, and physical areas of the Town.

2) Incident management responsibilities and procedures are established to ensure timely response to incidents.

3) The Town's IT team (Incident Responders) is established to handle the intake, communication, and remediation of security incidents.

    a. Incident responders must provide primary and secondary contact information so that they can be reached in the event of a relevant security incident.

    b. Incident responders will establish a method of communication alternative to the primary method that is to be used in the event that the primary communication

method is affected by, or is otherwise unavailable during, the security incident (e.g. cell phones).

c. Communication with affected parties will be provided on an as-needed basis until the incident is contained. It is up to the discretion of the incident responders to withhold information if the disclosure of said information deems a reasonable risk to the Town's security while the response is ongoing.

4) Information security events must be reported through the help desk. Incidents will be tracked as they occur. Any weaknesses, suspected or verified, in systems and services must be reported by users using those systems and services. End users should contact help desk by dialing 4357 or emailing helpdesk@taber.ca to submit a ticket.

5) As information security events are assessed, determinations are made about whether they can be identified as information security incidents. Once an event is deemed a true security incident, the incident will be classified as such and relevant incident responders will be notified.

6) Information security incidents will be identified and classified into different severity levels to make incident response process more effective.

7) In the event of a major incident, only a designated spokesperson will address the media. In the event that others need to speak to the media, guidelines for what can and cannot be stated must be provided not less than 24 hours before the scheduled media interaction.

8) After all relevant security incidents, a post-incident review will be conducted by incident responders to determine the root cause of the incident, the consequences, and the lessons learned. Information gained from responding to and resolving incidents will be used to reduce potential future incidents. Any affected parties, including end users, may be contacted for additional insight.

9) The incident response plan will be reviewed and, where applicable, revised on an annual basis. The review will be based on the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

10) Violations of this policy will be treated like other allegations of wrongdoing at the Town.

11) Administration shall establish procedures for this policy and shall be responsible to ensure the spirit and intent of the policy is adhered to.

Additional References

N/A

MAYOR — DATE: OCT. 7, 2020

CHIEF ADMINISTRATIVE OFFICER — DATE: Oct. 5/2020