IT Security Incident Management

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Review Date: September 2023	**Repealed Date:**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

Purpose

This procedure is intended to define a high-level incident response plan for any security incident. It is used to define general communication processes for managing security incidents, which may help minimize the impact and scope of the incident on the Town of Taber.

Operating Guidelines

1) The Town approach to incident response and management will follow the general guidelines in alignment with National Institute of Standards and Technology (NIST) SP 800-61 Rev. 2

2) During the detection phase, IT team will evaluate a potential security incident. Once an incident has been detected, a help desk ticket is opened to initiate the detection phase.

3) During the analysis phase, IT team will investigate the incident to determine the impact and scope of the threat. Depending on the impact and scope, a threat escalation tier level will be assigned, indicating the number of teams that will be involved in the remediation of the incident, and the notification of the threat will be escalated as appropriate. A third party may be involved if deep forensic analysis is needed.

4) During the containment phase, IT team will isolate and contain the incident to limit its ability to spread to the rest of the organization.

5) During the eradication phase, IT team will eliminate components of the incident, such as deleting malware and removing unauthorized user access, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

6) During the recovery phase, IT team will enact processes and procedures for recovery and full restoration of any systems, devices, or accounts during the incident. In recovery, responders will restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.

7) Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, re-issuing devices, and tightening network perimeter security (e.g. firewall rulesets, boundary router access control lists).

8) During the post-incident phase, IT team will perform root-cause analysis and lessons learned activities with various teams and stakeholders within the Town. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

CHIEF ADMINISTRATIVE OFFICER

Oct. 5/2020
DATE