Administrative Policy
2024-03-CS

Cybersecurity Incident Management

Effective Date	November 3, 2020
Approving Authority	Executive Leadership Team
Policy Owner	Director, Technology, Corporate Services

PURPOSE & SCOPE

Purpose

1 The purpose of this policy is to ensure proper recognition, management, and communication of cybersecurity events and weaknesses through a formal process.

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

Scope

3 This policy applies to:

(a) all authorized users,

(b) all technology assets, and

(c) both electronic and hardcopy information.

4 This policy does not apply to information owned by external parties. These groups are responsible for governing the collection and use of their own information.

POLICY PROVISIONS

Definitions

5 The following definitions apply to this policy:

5.1 Authorized user means an individual who has been granted access to use City of Regina technology assets. Authorized users may be employees, elected officials or external users, including the public, contractors, consultants or service providers working on behalf of the City.

5.2 Major cybersecurity incident means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information to the City or its information system(s).

5.3 Technology assets means all technology hardware, software and applications owned and operated by the City whether they are located on-premises, colocation facilities or cloud storage services.

Policy Statement

6 Incident management responsibilities and procedures are established to ensure timely response to major cybersecurity incidents.

7 The City's Technology department will appoint an incident response team to handle the intake, communication, and remediation of major cybersecurity incidents.

7.1 Incident responders as designated by the Technology department must provide primary and secondary contact information so that they can be reached in the event of a major cybersecurity incident.

7.2 Incident responders will establish an alternate method of communication for use in the event that the primary communication method, is affected by, or is otherwise unavailable during, the major cybersecurity incident.

7.3 Communication with affected parties will be provided on an as-needed basis, but not less than once every 24 hours until the major cybersecurity incident is contained. Incident responders will have the discretion to withhold information if the disclosure of said information is deemed to be a reasonable risk to the City's information technology (IT) systems while the response is ongoing.

8 The Technology department's cyber incident response capability will include a defined plan and address the seven stages of cyber incident response:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activity

9 Cybersecurity events must be reported to the Technology department, which will track incidents as they occur.

10 Any weaknesses suspected or verified in systems and services must be reported by authorized users using those systems and services. Authorized users should contact the Technology Service Centre by emailing techservicecentre@regina.ca or by dialing **306-777-7980** to submit a ticket.

11 As cybersecurity events are assessed, the Technology Service Centre will determine whether they can be identified as major cybersecurity incidents. Once an event is deemed

a major cybersecurity incident, the incident will be classified as such, and relevant incident responders will be notified.

12 Major cybersecurity incidents will be identified and classified into different severity levels to make the incident response process more effective.

13 Incidents will be responded to with the appropriate procedures established by the Technology department.

14 The Technology department will review its incident response procedures annually, and any required updates will be communicated to the appropriate parties.

15 In the event of a major cybersecurity incident, only a designated City spokesperson will address the media.

16 In the event that other City employees need to speak to the media, the Technology department will provide guidelines for what may be disclosed about the major cybersecurity incident at least 72 hours before the scheduled media interaction.

17 After every major cybersecurity incident, a post-incident review will be conducted by incident responders to determine the root cause of the incident, the consequences, and the lessons learned. The information gained from responding to and resolving incidents will be used to reduce potential future incidents. Any affected authorized user may be contacted for additional insight.

Related Documents

18 The Cybersecurity Incident Response Administrative Procedure is relevant to this policy.

Date Approved	November 2, 2020
Date of Last Review	December 20, 2023
Date of Next Review	December 20, 2025