Town of OLDS

204C
Incident Management

Supporting Procedure:

Prepared By: Finance

Council Approval Date: October 13, 2020

Effective Date:

Council Resolution No.: 20-389

References:
Personal Information Protection and Electronic Documents Act (PIPEDA), Sections 2, 6, 8
Payment Card Industry Data Security Standard (PCI-DSS), Sections 9.6, 9.7, 12
Records Management Retention Bylaw

POLICY STATEMENT

To ensure a consistent and effective approach to the management of Information Security Incidents, including communication on security events and weaknesses.

PURPOSE

This policy enables the efficient and effective management of Information Security Incidents by providing a definition of an Information Security Incident and establishing a structure for the reporting and management of such incidents.

SCOPE AND GUIDELINES

This policy applies to all Elected Officials, Employees and Contractors of the Town of Olds with reference to all information held by or on behalf of the Town of Olds.

DEFINITIONS

"Classified Information" is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature.

"Information Security Incident" An Information Security Incident is the occurrence or development of an unwanted or unexpected situation which indicates **either**:

a) a possible breach of information security controls **or**
b) a failure of information security controls which have a significant probability of compromising business operations.

Examples of Information Security Incidents include (but are not limited to):

- Direct loss or theft of Classified Information (e.g. papers taken from car, post intercepted, unauthorised download)
- Loss or theft of equipment used to store Classified Information (e.g. laptop, smartphone, USB stick)
- Accidental or unauthorised disclosure of 'Confidential' or 'Highly Confidential' Classified Information (e.g. via misaddressed correspondence or incorrect system permissions/filter failure)
- Corruption or unauthorised modification of vital records (e.g. alteration of master records)
- Computer system or equipment compromise (e.g. virus, malware, denial of service attack)
- Compromised IT user account (e.g. spoofing, hacking, shared password)
- Break in at a location holding Classified Information or containing critical information processing equipment such as servers

"Serious Information Security Incident" is an incident whose impact, if unmanaged, has the potential to affect business as usual for the Town of Olds.

RESPONSIBILITIES

The Chief Administrative Officer (CAO) or designate(s) is responsible for administering this policy within the standards established.

STANDARDS

Information Security Incidents shall be reported promptly and responded to in a quick, effective and orderly manner to reduce the negative effect of incidents, to repair damage and to inform policy and mitigate future risks.

- All Elected Officials, Employees and Contractors of the Town of Olds are responsible for reporting actual or suspected Information Security Incidents to the Director of Finance as soon as possible.
- The Director of Finance or designate shall report all Information Security Incidents promptly to the Town of Olds external IT support.
- The severity of each incident shall be assessed, and the management response shall be proportionate to the threat.
- Records about all Information Security incidents, including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analysed to assess the effectiveness of information security controls.
- New risks identified as a result of an incident shall be communicated to the Director of Finance and unacceptable risks shall be mitigated promptly.
- Contractors using the Town of Olds information systems and services shall be required to note and report any significant information security weaknesses in those systems or services.
- The responsibility for reporting Serious Information Security Incidents to external authorities lies with the Director of Finance Failure to report an Information Security Incident and any other breach of this policy shall be considered to be a disciplinary matter and shall be reported to the Director of Finance.
- Compliance with this policy should form part of any contract with a third party that may involve access to the Town of Olds networks, computer systems or data. Failure by contractors to comply with this policy may constitute an actionable breach of contract.