Information Technology	Administrative Guideline
Title:	**Information Security Standards Questionnaire**
Date in Effect:	March 31, 2025

Section 1: Document Scope

Context

This questionnaire is designed to assess the information security measures applicable to contractors or any third parties providing The Town of Canmore with goods or services that includes an information technology component. These standards apply to the handling of data or information acquired electronically by the Contractor from the Town or other persons in relation to the delivery of the goods or services to the Town. This document is not a list of requirements, rather it is a questionnaire to help us assess the security features of the product provided.

Definitions

- "Contractor" means any person or entity engaged by agreement to provide goods or services to the Town, regardless of reference to this person as a contractor, vendor, supplier, consultant, or service provider under the applicable agreement.
- "Services" means any goods or services provided by the Contractor to the Town under the agreements by which the Contractor is engaged by the Town.
- "Town" means the Town of Canmore.
- "Town data" or "Town information" means data or information obtained by Contractors through delivery of the Services to the Town, including but not limited to personal information as defined by legislation.

Evalution

For the purposes of RFP evaluations regarding security. Other factors outside of the scope of this document may also affect evaluations. Each response will be given a weight based on these sections:

- Section 2 will be weighted for 40 points
- Section 3 will be weighted for 60 points
- Section 4 will be weighted for 60 points

Section 2: Core Factors

This section relates to items the Town would be interested in regardless of the answers in sections 3 and 4. Please fill out the questions to the best of your abilities.

1. Contractor Contact information for Security/Software based concerns:
   - ☐ ____
2. Do you provide an Azure Single-Sign On (SSO) Integration? (7 points)
   - ☐ Yes
   - ☐ No
   - ☐ If so, does integration support SCIM (2 points)
3. Will the implementation and/or maintenance of the proposed solution require the Town to maintain internal (Town) accounts to access (i.e. VPN, Windows Logins, O365 Logins, etc.) (7 points)
   - ☐ Yes
   - ☐ No
4. Does the contractor solution have the ability to provide a complete download of all Town data (10 points)
   - ☐ Yes
   - ☐ No
5. Location of Data Hosting (Country or Region): ____________ (7 points)
   - ▪ If outside Canada or if Private Information is involved, there may be an additional assessment required
6. Provide documentation related to SLA and uptime guarantees if applicable. (7 points)

Section 3: Existing Security Standards

1. Do you currently adhere to any existing security standards such as ISO/IEC 27001, SOC2, or others? (55 points)
   - ☐ Yes
   - ☐ No
2. If yes, please provide any relevant documentation or link to your policy (5 points)

3. If there are any documented exceptions, please note them

Section 4: Security Checklist

If you responded "Yes" to Section 3 Question 1, you may skip Section 4 and continue to Section 5. Otherwise, please tick any boxes that apply to assess the information security measures applicable to your solution. These questions will be in reference to the Contractors Processes/Procedures unless otherwise specified.

Contractor Account Management

- □ MFA on administrative accounts (2 points)
  - □ MFA when Accessing Town data (2 points)
- □ Role-Based Access Control (RBAC) best practices for data access (4 points)
- □ Sole-Authorized Accounts (Each user gets a separate login) (4 points)

Vulnerability and Data Management

- □ All systems and software remain up to date and licensed (4 points)
- □ Remediate any high-risk vulnerabilities within 30 days of disclosure of the vulnerability (considered to be high risk when Private or Town data can be accessed or exfiltrated) (4 points)
  - □ If not 30 days: ___________
- □ Data in transit and Data at rest is encrypted with TLS 1.2 or equivalent (4 points)
- □ Physical Security measures are in place to prevent unauthorized access to data (4 points)

Business Continuity

- □ Ensure data is backed up and recoverable. (4 points)
  - □ Alternatively, ability for the Town to maintain backups (4 points)
- □ Do you have any disaster management/mitigation plans in place to minimize outage windows with relation to the services provided to the Town. (4 points)
  - □ If possible, please link to said documents or policies

Logging

- □ Log interactions with Town Data (2 points)
  - □ What is the duration of log retention: ___________ (2 points)
- □ Do you maintain and monitor logs for the purposes of identifying and mitigating potential security risks (4 points)

Email

- □ Do you support Modern Email Protocols (DMARC, DKIM, SPF, etc.) (4 points)
- □ Modern authentication when sending emails via M365 (4 points)
- □ Support authenticated SMTP if on premise (4 points)

Section 5: Document Management

- Changes to this Guideline may be requested by contacting the Manager of Information Technology.
- The Municipal Clerk’s Office is responsible for maintaining the recorded copy of this Guideline.

Created by: Garrett Irwin
Enterprise Solutions Architect Date: March 31, 2025

Revision History

Action	**Date**	**Notes**
Approved	March 31, 2025	Initial Document Creation

Contractor Signature

Name Printed	
Job Title	
Signature	
Date	