Security Schedule Guide

Audience & purpose

The purpose of this document is to help B.C. government Ministry Information Security Officers (MISOs) and their Legal Services Branch representatives to better understand the clauses in the Security Schedule. Security Schedule can be found in the BC Government Contract templates appendices.

This document is intended for internal use only.

Introduction

The Security Schedule outlines the security requirements that a Contractor must adhere to to safeguard B.C. government systems and information. It defines the minimum security controls for information classified as 'Protected B' or lower (refer to IMIT 6.18 Information Security Classification Standard) and for systems that are not critical to government service delivery (see IMIT 5.10 Critical Systems Standard).

The Security Schedule must always be attached to a contract. While the Security Schedule can be modified, any changes must be reviewed and approved by both the Ministry Legal Counsel and the Ministry Information Security Officer (MISO).

Rules of Use

When procuring a product or service, always begin with security a Security Threat and Risk Assessment (STRA) and Privacy Impact Assessment (PIA). Once these assessments are completed, you will have a clearer understanding of whether the Security Schedule should be modified. Refer to IMIT 6.30 Supplier Relationships Security Standard for additional guidance.

If ministries need to modify any sections because the Contractor cannot comply with them, their MISO should first:

1. Talk to their legal representative about it.
2. Assess the modifications through STRA and ensure adequate security controls are applied.

Ask for guidance and help Please contact ociosecurity@gov.bc.ca for further advice.

Section 1 - Definitions

The purpose of this section is to provide a common understanding of the terms used in the contract to reduce confusion. The definitions are aligned with the General Services Agreement (GSA) and Privacy Schedule to help improve the overall enforceability of the contract.

Sections 2 - 5 - Interpretation and Applicability

The purpose of this section is to clarify how to read the Security Schedule and explain where it applies. These sections hold the Contractor accountable for the security of the IM/IT products or services they are offering as part of the contract, and for any sub-contractors they may use in contract delivery.

Section 6 - Expectation of Standards

The purpose of this section is to reduce supply chain risks that may be introduced through use of sub-contractors by the Contractor in the delivery of the contract. This section requires the Contractor to also ensure any sub-contractor they use meets or exceeds the requirements set out in the Security Schedule. See also IMIT 6.30 Supplier Relationships Security Standard.

Section 7 – Industry Best Practice

The purpose of this section is to ensure security concerns and controls that are not explicitly listed elsewhere in the schedule are addressed.

Industry Best Practice refers to well-known cybersecurity practices relevant to the product or service(s) offered. Organizations like the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), Open Worldwide Application Security Project (OWASP) publish best practices for the information security industry. The industry sector, for example, the payment card industry, have some more specific well-known practices like the Payment Card Industry Data Security Standard (PCI DSS).

Sections 8 - 9 – Compliance and Certifications

The purpose of these sections is to ensure that the Contractor applies security controls and practices acceptable to the Province for the IM/IT product or service the Contractor offers. These sections identify the acceptable security certifications or compliance profiles that verify and validate the Contractor is applying best cybersecurity practices. The

security certification or compliance profile reduces the scope of the STRA and simplifies the STRA process.

Note: An acceptable security certification or compliance profile for the Contractor's IM/IT product or service does not automatically guarantee that the Province and ministry security requirements will be met. Ministries must still ensure their security requirements are met.

If the Contractor has a security certification or compliance profile other than those listed in the Security Schedule for their IM/IT product or service, they must be able explain how the certification or compliance profile maps to the required certifications or compliance profile. For example, if the Contractor only has SOC 2 Type 2 report, they need to present the scope of the assessment and explain how the security controls they have implemented meet the requirements listed in the Security Schedule. Ministries must review these explanations and ensure B.C. government and ministry security requirements are met.

If the Contractor has no security certification or cannot provide a recent SOC 2 report, ministries must ensure the Contractor follows the security practices and controls outlined in the B.C. government's IM/IT security standards.

Section 10 – Attestation of Compliance and Certification of Services

The purpose of this section is to ensure the Contractor continues to have good security controls and practices for the IM/IT product or service for the contract term. Provision of an independent third-party attestation for the claimed security certification or compliance profile on a regular basis verifies this.

Sections 11 - Access Control

Access control and authentication requirements are core security controls. Requirements listed in the Security Schedule are high level. More detailed requirements can be found in the IM/IT security standards and specification, see IMIT 6.24 Access Control Security Standard. Weak access and authentication controls will result in increased risk of exposure to Province Information.

This section ensures the Contractor implements the minimum access and authentication security controls and practices. If the Contractor has a security certification or compliance profile listed in sections 8 – 9, the requirements in this section are typically covered. If the Contractor does not have the required certifications, these sections state the minimum security requirements the Contractor must meet.

Sections 12 - Authentication

Authentication requirements are tightly related to Access Control requirements and are core security controls. Requirements listed in the Security Schedule are high level. Weak authentication controls will result in increased risk of exposure to Province Information.

This section ensures the Contractor implements the minimum access and authentication security controls and practices. If the Contractor has a security certification or compliance profile listed in sections 8 – 9, the requirements in this section are typically covered. If the Contractor does not have the required certifications, these sections state the minimum security requirements the Contractor must meet.

Ministries should always ensure any modifications to these sections enables their compliance with the Information Security Policy (ISP) and the IMIT 6.24 Access Control Standard.

Section 13 – Security Awareness

Security awareness training promotes a security-conscious culture in an organization and reduces the risk of personnel falling for phishing and scams. It is usually a component of a robust information security program an organization implements for a strong security posture.

The purpose of this section is to reduce security risks to the Province from Contractor personnel with no security awareness training. Contractors that provide security awareness training to staff are also likely to have implemented an information security program to increase their organization's security posture.

Ministries should do business only with Contractors who have a strong security posture.

Section 14 - Logging

The purpose of this section is to ensure the Province is not hampered by insufficient or lack of access to logs generated on the Contractor's IM/IT products or services in its efforts to:

1. Monitor the security of Province Information and systems.
2. Respond to incidents for response purposes.

This section requires the Contractor to implement sufficient logging, and provide the Province timely access to the logs. In some situations, real time (or close to real time) access to logs may be required; in others, logs provided via batch processing may be acceptable.

Ministries must:

1. Ensure the Contractor can meet their logging requirements and the Province's assessed during the STRA for the program or initiative that will be enabled by the contract delivery. See the following standards for Province logging requirements:
   - IMIT 6.14 Application and Web Security Standard
   - IMIT 6.15 Mobile Device Management Security Standard
   - IMIT 6.16 Database Security Standard
   - IMIT 6.24 Access Control Standard
   - IMIT 6.26 Physical and Environmental Security
   - IMIT 6.27 Operations Security Standard
   - IMIT 6.28 Network and Communications Security Standard
2. Document the logging needs in the SOW.

Ministries may need to make separate arrangements to retain the logs for durations specified in the ARC and ORCs records retention schedules (6820 - Information Systems Operations - Province of British Columbia (gov.bc.ca)).

Section 15 - Investigations

The purpose of this section is to ensure the Contractor is prepared to:

1. Provide support to the Province for the Province's investigations
2. Safeguard Province Information from access by jurisdictional authorities (local or foreign) when not legally obligated to do so.

Example: A U.S. Contractor operating in Canada is legally obligated to release Province Information to a U.S. authority on request even without written permission from the Province. However, they are not legally obligated to release Province Information to a local authority like the RCMP without written permission from the Province or a court order.

Section 16 – Development, Configuration, Vulnerability management

The purpose of this section is to ensure that the Contractor applies reasonable security practices when developing or managing systems. Weak or non-existent security practices will result in increased security risks for the Province and ministries.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9, the requirements in this section are typically covered. If the Contractor does not have a required certification or compliance profile, this section states the minimum security requirements the Contractor must meet.

Ministries should ensure any Contractor follows applicable IM/IT security standards if:

1. They help develop or manage a Province system.
2. They do not have a required certification or compliance profile for the IM/IT products or services they provide

Ministries should always ensure any modification to this section still enables their compliance with:

- IMIT 6.14 Application and Web Security Standard
- IMIT 6.16 Database Security Standard
- IMIT 6.24 Access Control Standard
- IMIT 6.27 Operations Security Standard
- IMIT 6.28 Network and Communications Security Standard
- IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard

Section 17 - Business Continuity / Disaster Recovery

The purpose of this section is to ensure the Contractor's ability to deliver on the contract is not impacted by a disaster that disrupts their business operations. Disruptions in the delivery of the contract may disrupt Ministries' program or service delivery that is dependent on the contract.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9, the requirements in this section are typically covered. If the Contractor does not have the required certifications, this section states the minimum security requirements the Contractor must meet.

Ministries should ensure their availability requirements are met by the Contractor's Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the contracted product or service. See also IMIT 6.16 Database Security Standard.

Section 18 – Incident response

The purpose of this section is to ensure the Contractor can effectively manage and contain incidents that may disrupt their business operations and the delivery of the contract. Disruptions in the delivery of the contract may disrupt ministries' program or service delivery that is dependent on the contract.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9, the requirements in this section are typically covered. If the Contractor does not have the required certifications, this section states the minimum security requirements the Contractor must meet.

Ministries will need to initiate and coordinate their incident response with the Contractor if Province Information or system was impacted by the incident.

Ministries should ensure any modifications to this section still enables their compliance with IMIT 6.31 Cybersecurity Incident Management Standard and Section 19.

Section 19 – Notification of Incidents

The purpose of this section is to ensure the Province can be compliant with Freedom of Information and Protection of Privacy Act -(FOIPPA) and respond to an incident in a timely manner. If a privacy breach resulted from the incident, the Province is required to notify without unreasonable delay the affected individual(s) and the Office of the Information Privacy Commissioner (OIPC) if the individual(s) are reasonably expected to be affected by significant harm.

The 24-hour notification period is considered reasonable to enable the Province to:

1. Respond to the incident as appropriate.
2. Notify the affected individuals (if necessary) and the OIPC without unreasonable delay if a privacy breach resulted from the incident.

If a privacy breach has occurred as a result of the incident, ministries must follow the Information Incident Management Policy. The Corporate Information and Records Management Office (CIRMO) will assess the level of harm resulting from the incident to affected individuals to determine if a privacy breach notification is required.

Ministries may allow a longer notification period if the Contractor cannot comply with the 24-hour notification period. Ministries should first talk to their MISO and legal representative if they need to modify this section of the Security Schedule.

Section 20 – Notification of Changes

The purpose of this section is to ensure the Contractor notifies Province about any changes that may weaken their security posture, and thereby, the security of the contracted service. A Contractor's weakened security posture increases risk of Province Information exposure or loss.

Section 21 – Asset Management and Disposal

Province Information is an asset to be managed securely. The purpose of this section is to ensure Province Information managed or handled by the Contractor is secured against the risk of information loss or exposure. Ministries must ensure all Province Information in the custody of the Contractor is:

1. Properly accounted for. Province Information not accounted for is at risk of loss or exposure.
2. Returned in a usable state (if the information was stored in a proprietary format). Province Information returned in an unusable state is considered a loss of Province Information.
3. Disposed of securely at the end of the contract (this particularly refers to backed up copies of Province Information) or on request. Province Information not erased securely from storage media is at risk of exposure.

Ministries should ensure any modifications to this section still enables their compliance with IMIT 6.23 Asset Management Security Standard.

Section 22 – Physical Security

The purpose of this section is to ensure the physical location where Province Information is managed or handled by the Contractor has the appropriate controls to prevent physical loss, theft, or damage to Province Information from lack of or weak physical and environmental controls and practices. Province Information can be lost or corrupted when the storage media used to store Province Information is lost or damaged from excess moisture, heat, vandalism, or theft. See IMIT 6.26 Physical and Environmental Security.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9 for the information system, platform, application, or IT service, the requirements in this section are typically covered.

If the Contractor does not have a required certification or compliance profile, this section sets the minimum security requirements. Ministries must define when requirement 22 (c) is applicable.

Note: Access logs for sites where Contractor systems may be physically located and accessed by multiple Contractor personnel, for example, telecommunication or network hub sites, data centres, offices must be maintained. Access logs for sites where individual Contractor personnel may physically conduct remote work from, for example, their homes, are not required.

Section 23 - STRA

The purpose of this section is to ensure the Contractor:

1. Has proper security risk management practices in place.

2. Is willing to provide the necessary information to assist ministries in their STRAs on the contracted product or service.

Security risks not properly identified managed increases risk for the Province and ministries. Ministries should first talk to their MISO and legal representative if they need to modify this section of the Security Schedule.

Section 24 - Security Screening

Security screening is a component of an information security program that increases the security posture of any company or team. It ensures any personnel hired is who they claim to be and has the required skills to do the job they are hired to do. Ministries must ensure that Contractor personnel do not pose a risk to Province Information or Province Systems as an employee who:

- Is an imposter (for example: https://www.bbc.com/news/articles/ce8vedz4yk7o).
- May be susceptible to external coercion.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9 for the information system, platform, application, or IT service, the requirements in this section are typically covered. If the Contractor does not have the required certifications, this section states the minimum security requirements the Contractor must meet.

Section 25 - Encryption

The purpose of this section is to ensure Province information is protected against unauthorized access through the Contractor's information system, platform, application, or IT service. Encryption and control of access to the encryption keys are security access controls. Contractors who have access to the encryption keys to encrypted Province Information can be forced by foreign authorities to provide unauthorized access to Province Information.

Ministries can remove Sections 25 (b) and 25 (c) if the risks to Province information **do not increase** when the Contractor manages the encryption keys.

Ministries should consider modifying this section to require the Contractor to use quantum-resistant encryption if the confidentiality or integrity of Province information must preserved beyond 2030.

Section 26 - Isolation

The purpose of this section is to ensure Province Information is not accidentally affected or exposed when a shared infrastructure is part of the Contractor's information system,

platform, application, or IT service. On a shared infrastructure, Province Information is at risk of exposure if it is not properly isolated from Contractor information or their other clients.

Ministries should always include this section as the security certification or compliance profile listed in sections 8 - 9 do not include this requirement.

Section 27 - Network Controls

The purpose of this section is to ensure the risk of unauthorized access to Province Information or exposure from weak or lack of network controls for the Contractor's information system, platform, application, or IT service is minimized.

If the Contractor has a security certification or compliance profile listed in sections 8 – 9 for the information system, platform, application, or IT service, the requirements in this section are typically covered. If the Contractor does not have the required certifications, this section states the minimum security requirements the Contractor must meet.

Examples of technical security controls: Network segmentation, firewalls, web application firewalls, distributed denial of service protection systems, intrusion prevention systems, encrypted communications.

Examples of applicable security controls: Constant monitoring for unusual network activity, alerting, response.

Ministries should ensure the modifications to this section still enables their compliance with IMIT 6.13 Network Security Zones Standard and IMIT 6.28 Network and Communications Security Standard.

Section 28 - Use of Province Systems

The purpose of this section is to remind the Contractor that when they are granted access to Province systems, they can use them only for the purposes necessary for the delivery of the contract.

Ministries should always include this section as the security certification or compliance profile listed in sections 8 - 9 do not include this requirement.

Section 29 - Security Contact

Per IMIT 6.31 Cybersecurity Incident Management Security Standard, the purpose of this section is to ensure ministries have a contact in the Contractor's organization to coordinate incident management and other security activities when needed.

Ministries should always include this section as the security certification or compliance profile listed in sections 8 - 9 do not include this requirement.

Section 30 - Record Keeping

The purpose of this section is to ensure the ministries and the Province:

1. Better understand how well the Contractor is managing security risks to Province Information and Province Systems.
2. Be compliant with FOIPPA.

Ministries should always include this section as the security certification or compliance profile listed in sections 8 - 9 do not include this requirement.

Section 31 - Survival

The purpose of this section is to ensure that the Contractor takes proper care of Province information until it is permanently erased (the erasure might happen after the contract ends).

Ministries should always include this section as the security certification or compliance profile listed in sections 8 - 9 do not include this requirement.