[This Schedule must be used if the Contractor will be required under the Agreement to either

(1) treat any information as confidential; or
(2) preserve the integrity or availability of any record.

This Schedule must be used without modification unless Ministry legal counsel drafts or advises on the modification. In addition, the Ministry Information Security Officer or, if the Services are for shared services, the OCIO Information Security Branch, must approve any modification proposing:

(1) alternate security requirements, which in any event must be warranted and not introduce indefensible information security risk; or
(2) additional obligations (for example, enhanced security screening, or for particularly sensitive personal information), and if they are to be included in the Security Schedule should be attached as an Exhibit.

For guidance related to this Schedule, please contact the OCIO at OCIOSecurity@gov.bc.ca.

All bracketed instructions must be deleted.]

SECURITY SCHEDULE
February 2020

If a provision of the main body of the Agreement conflicts with a provision of this Schedule, then unless expressly stated otherwise within the Agreement, the provision of this Schedule will prevail to the extent of such conflict.

1 Definitions

In this Schedule,

(a) "**Cloud Services**" means services made available to users on demand via the Internet that are characterised by resource pooling, rapid elasticity and measured services with broad network access. Cloud Services include Software as a Service, Platform as a Service and Infrastructure as a Service, as such terms are understood pursuant to definitions provided by the National Institute of Standards and Technology (NIST).

(b) "**Industry Best Practice**" means best practices commonly recognized in the IT industry from time to time and applicable to the protection and security of sensitive information of a nature similar to Protected Information against unauthorised access, disclosure or use, or any unauthorized attempts to access, disclose or use such information.

(c) "**Protected Information**" means any and all of:

i. "personal information" as defined in the *Freedom of Information and Protection of Privacy Act,* British Columbia;

ii. information and records of information the Contractor is required to treat as confidential under the Agreement; and

iii. records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked by the Province as "Protected Information" or

the Province otherwise instructs the Contractor that the record is "Protected Information" under the Agreement.

(d) **"Province Information**" means information of the Province, including without limitation any Protected Information, that is disclosed to the Contractor, accessed by the Contractor or collected by the Contractor in relation to the Services and includes any information derived therefrom.

(e) **"Services"** means the services provided by the Contractor to the Province under the Agreement and includes, if applicable, any Cloud Services.

(f) "**Systems"** means any systems, subsystems, equipment, devices, infrastructure, networks, hardware and software used in connection with the Services, including for managing, operating or providing the Services.

2 Applicability

For greater clarity, unless otherwise specified in the Agreement, the terms and conditions of this Schedule apply to the provision of all Services by the Contractor, its subcontractors and their respective personnel. Any reference to Contractor herein will include all subcontractors, Contractor personnel and subcontractor personnel, as applicable.

3 Industry Best Practice

The Contractor must have in place and maintain security controls to protect Protected Information that conform to commonly accepted industry norms that a prudent operator providing similar services would have implemented. Without limitation, the Contractor will perform its obligations under this Schedule in a manner that best conforms to Industry Best Practice.

4 Compliance and Certifications

Compliance and certification requirements will depend on the type of service provided by the Contractor.

(a) For Cloud Services, the Contractor must at all times satisfy at least one of the following security standards:

i. compliance requirements identified for a Cloud Service Provider, in the Government of Canada Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM); or

ii. compliance requirements identified for a Cloud Service Provider, in the US Federal Risk and Authorization Management Program (FedRAMP) for moderate impact information systems; or

iii. certification with ISO/IEC 27001 based on requirements for a Cloud Service Provider controls in ISO/IEC 27017:2015; or

iv. certification with Cloud Security Alliance (CSA) – Level 2 CSA STAR;

(b) For all other Services that are not cloud services, the Contractor must satisfy:

i. certification with ISO/IEC 27001 based on requirements for Information Technology controls in ISO/IEC 27002:2013; or

ii. applicable Province IM/IT standards accessible at

https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards

5 Attestation of Compliance and Certification of Services

To verify compliance with, as applicable, section 4(a) (with respect to Cloud Services) or 4(b) (with respect to non-Cloud Services), the Contractor must provide the Province with satisfactory evidence, by way of independent third-party attestation from a reputable information systems auditor, that any Services provided by the Contractor or used by the Contractor in connection with the Services satisfy and comply with at least one of the security standards set forth in, as applicable, section 4(a) (with respect to Cloud Services) or 4(b) (with respect to non-Cloud Services).

6 Access Control

With respect to the access, by any Contractor personnel, to any part of the Contractor's Systems that may contain Province Information, the Contractor must:

(a) implement access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts;

(b) identify and segregate conflicting duties and areas of responsibility, such as separation of duties;

(c) maintain a current and accurate inventory of computer accounts;

(d) review the inventory of computer accounts on a regular basis to identify dormant, fictitious or unused accounts;

(e) enforce principles of "least privilege" and "need to know";

(f) review user access rights on a regular basis to identify excessive privileges;

(g) enforce a limit of logon attempts and concurrent sessions.

7 Authentication

Where the Contractor manages user authentication controls for Contractor personnel, the Contractor must:

(a) enforce minimum password complexity, such as requiring passwords to be case sensitive, or requiring passwords to contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;

(b) require regular change of passwords at predetermined intervals, and which limit reuse; and

(c) require multi-factor authentication for privileged access.

8 Security Awareness

(a) The Contractor must ensure that all persons employed or retained to perform the Services receive security awareness training, annually and supervision at a level and in substance that is appropriate to that person's position and the Contractor's obligations under this Schedule.

(b) The Contractor must not permit any person the Contractor hires or uses to access

or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under the Agreement.

9 Log Generation and Retention

The Contractor must:

(a) generate and retain logs that are sufficiently detailed to determine who did what and when for a period of 90 days online;

(b) provide real time access to logs;

(c) provide the technical capability to forward the logs to the Province; and

(d) correlate, monitor, and alert on logs.

10 Investigations Support and Security Investigations

The Contractor must:

(a) retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to the Province for retention;

(b) provide reasonable investigative support to the Province;

(c) maintain chain of custody for evidence;

(d) support e-discovery; and

(e) maintain legal holds to meet needs of investigations and judicial requests.

11 Network Time Protocol

Systems used by the Contractor or any subcontractor in the provision of Services must synchronise time with a stratum-2 (or higher time) reliable source.

12 Vulnerability Scan/Penetration Testing

The Contractor must conduct regular:

(a) vulnerability scans;

(b) web application scans; and

(c) penetration tests.

13 Configuration and Patch Management

The Contractor must:

(a) have an information security policy based on recognized industry standards;

(b) apply system hardening methods in securing Contractor Systems;

(c) logically isolate and encrypt Province Information;

(d) ensure workstations and servers used in management and provisioning of the Services are patched and secured with anti-malware protection;

(e) remedy vulnerabilities in a timely manner according to criticality;

(f) patch all systems and software regularly according to industry best practices; and

(g) use secure coding practices when developing applications and application programming interfaces.

14 Business Continuity, Disaster Recovery, and Backup Plans

The Contractor must:

(a) have a business continuity plan and a disaster recovery plan;

(b) conduct backups of critical data; and

(c) review and test business continuity, disaster recovery, and backup plans and procedures regularly.

15 Incident Response and Management

The Contractor must:

(a) have an incident management plan and an incident response plan; and

(b) review and test both incident management and incident response plans annually.

16 Notifications of Breaches

The Contractor must notify the Province within 24 hours of the Contractor's identification of a breach or incident that has affected, or may affect, Province Information.

17 Notifications of Changes

The Contractor must notify the Province of any changes to the Contractor's security policies, procedures or agreements that may materially lower the security of Province Information.

18 Asset Management and Disposal

The Contractor must

(a) maintain an inventory of Province Information assets;

(b) use secure methods when disposing of Province Information Assets, and

(c) maintain records of Province Information asset disposals.

19 Physical Security

The Contractor must:

(a) develop, document, and disseminate a physical and environmental protection policy;

(b) regularly review and update its current physical and environmental protection policy and procedures; and

(c) review physical access logs at least once monthly.

20 Threat and Risk Assessments

The Contractor must:

(a) conduct threat and risk assessments on any part of the Contractor's Systems that is new, or has been materially changed since the last threat and risk assessment

was conducted; and

(b) support the Province in completing Security Threat and Risk Assessments.

21 Security Screening

The Contractor must:

(a) screen all Contractor personnel prior to Contractor authorizing access to Province or Contractor Systems;

(b) conduct criminal record checks on all Contractor personnel who have access to any Province or Contractor Systems;

(c) make a reasonable determination of whether the individual constitutes an unreasonable security risk taking into consideration the duties of the individual, the type and sensitivity of information to which the individual may be exposed, and all applicable laws; and

(d) require all Contractor personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law.

22 Supply Chain

The Contractor must ensure that its suppliers and subcontractors involved in the provision of Services meet or exceed the standards set forth in this Schedule.

23 Encryption

The Contractor must:

(a) implement and maintain encryption of Province Information while at rest and in transit;

(b) offer the Province the technical capability of cryptographic key management to allow the Province to manage encryption keys in relation to Province Information at rest and in transit;

(c) not hold or have access to encryption keys if such encryption keys are managed by the Province to encrypt Province information at rest or in transit; and

(d) not provide encryption keys used to secure Province Information to a third party or the ability to break such encryption.

24 Isolation Controls and Logical Isolation of Data

The Contractor must:

(a) implement and maintain the logical isolation of Province Information, even in the case of equipment or technology failure;

(b) implement, where supported by available technology, the logical isolation of audit records related to Province Information and activities, even in the case of equipment or technology failure; segregate tenancy traffic from management network traffic; and

(c) not use Protected Information for test or development purposes without the written approval of the Province.

25 Technical Controls

The Contractor must:

(a) implement firewalls, web application firewalls, distributed denial of service, and intrusion prevention systems to control traffic flow to and from the Contractor's Systems; and

(b) secure remote access to the Contractor's Systems by Contractor personnel and contractors.

26 Use of Province Systems

Use of Province Systems by the Contractor or its personnel (including subcontractors) must be restricted to activities necessary for provision of the Services. The Province reserves the right to not make any particular Province facility, system, network or device available to the Contractor unless the Contractor or its individual personnel (as applicable) agree to any additional terms and conditions acceptable to the Province.

27 Security Contact

If not set out elsewhere in the Agreement, the Contractor must provide the contact information for the individual who will coordinate compliance by the Contractor on matters relating to this Schedule.