Annex A
Schedule 1 – Security Obligations
for Tier 2 (up to and including Protected B) SaaS

1. General

1.1 Purpose

The purpose of this Schedule is to set forth the obligations of the Contractor relating to the proper management of Canada's Data, including protection from unauthorized modification, access or exfiltration, in accordance with the Agreement, this Schedule, and the Contractor's Security Measures (collectively, the "**Security Obligations**").

1.2 Flow-Down of Security Obligations

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Sub-processors and/or Subcontractors to the extent applicable.

1.3 Change Management

The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Requirements as needed to comply with the security best practices and industry standards as set forth in this Schedule.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse effect to the Cloud Services offerings in this Contract, including technological, administrative or other types of changes or improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgments

The parties acknowledge that:

(a) Canada's Data is subject to these Security Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Canada's Data.

(c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(d) Security Obligations apply to Tier 2 (up to and including Protected B / Medium Integrity, Medium Availability or Medium Injury), unless otherwise specified.

3. Securing Canada's Data

(1) The Contractor must protect Canada's Data from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate technical and organizational security measures including information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Canada's Data.

4. Roles and Responsibilities for Security

(1) The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the Cloud Services between the Contractor and Canada. This includes, at a minimum, the roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.

(2) The Contractor must provide to Canada an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there are significant changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of Canada.

5. Third-Party Assurance: Certifications and Reports

(1) The Contractor must ensure that Canada's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured with appropriate security measures that comply with the requirements set forth in the Contractor's security practices and policies.

(2) The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications and audit reports by providing independent third party assessment reports or certifications that addresses each service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering, including:

(a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; AND

(b) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body; AND

(c) AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing

integrity, and confidentiality - issued by an independent Certified Public Accountant.

(3) Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If there are any exclusions identified, or there is a need to separate a subservice organizations such as data centre hosting, the subservice organization's assessment report must be provided.

(4) Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

(5) Each SOC 2 Type II audit report must have been performed within the 12 months prior to the start of the contract. A bridge letter may be provided to demonstrate that the Contractor
is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

(6) The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and SOC 2 Type II for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

6. Auditing Compliance

(1) The Contractor must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Canada's Data as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by independent, third party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(2) Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings

by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(3) Upon request of Canada, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

7. Cloud Service Provider (CSP) IT Security Assessment Program

(1) The Contractor must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) (https://www.canada.ca/en/government/system/digital-government/modern-emergingtechnologies/cloud-computing/government-canada-security-control-profile-cloud-based-itservices.html) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

(2) Compliance will be assessed and validated through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

The Contractor must demonstrate that they participated in the process by successfully on-boarded, participated in, and completed the program. This includes providing the following documentation:

(i) A copy of the confirmation letter that confirms that they have on-boarded into the program;
(ii) A copy of the most recent completed assessment report provided by CCCS; and
(iii) A copy of the most recent summary report provided by CCCS.

The Contractor should contact the CCCS Client Services for any additional information related to the CSP IT Assessment Program.

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify CCCS when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

certifications identified below, and validated through independent third party assessments.

(3) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 5 - Third-Party Assurance and Section 7 - Cloud Service Provider (CSP) IT Security Assessment Program, ub-sections (1) and (2) the SaaS provider must provide Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Bidder has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a final report with regards to the assessment. For any questions, CCCS can be contacted by email at contact@cyber.gc.ca.

8. Data Protection

(1) The Contractor must:

(a) Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 13 - Cryptographic Protection.

(b) Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with Section 13 - Cryptographic Protection and Section 21- Network and Communications Security.

(c) Implement security controls that restricts administrative access to Canada's Data and Systems by the Contractor and provides the ability to require the approval of Canada before the Contractor can access Canada's Data to perform support, maintenance or operational activities.

(d) Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to Canada's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or customer support, based on approval from Canada.

(2) The Contractor must not make any copies of databases or any part of those databases containing Canada's Data outside of regular service resilience capabilities and within approved regional spaces or zones within Canada.

(3) The Contractor must ensure that any processing performed outside of Canada including moving or transmitting approved copies of data are performed within the agreed upon service regions.

(4) Upon request of Canada, the Contractor must provide Canada with a document that describes all additional metadata created from Canada's Data.

9. Data Isolation

(1) The Contractor must implement controls to ensure appropriate isolation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Cloud Services and Contractor Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

(a) The separation between Contractor's internal administration from resources used by its customers;

(b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and

(c) Ability for the GC to support isolation within GC-managed tenant environment.

(2) Upon request of Canada, the Contractor must provide Canada with a document that describes the approach for ensuring appropriate isolation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit.

10. Data Location

(1) The Contractor must store and protect Canada's Data, at rest, including data in backups or maintained for redundancy purposes. This includes the ability to isolate data in Canada in approved data centers. An approved Data Centre is defined as the following:

(a) A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security;

(b) Ensures the infeasibility of finding a specific customer's data on physical media; and

(c) Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 13 - Cryptographic Protection.

(2) The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European

Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries with which
Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(3) The Contractor must have the ability for Canada to isolate Canada's Data hosted in Cloud Services in data centers that are geographically located in Canada.

(4) Upon request of Canada, the Contractor must:

(a) Provide the GC with an up-to-date list of the physical locations, including city, which may store Canada's Data at rest; and

(b) Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

(5) It is the continuous obligation of the Contractor of the proposed Cloud Services to notify Canada when there are updates to the list of physical locations which may store Canada's Data at rest.

11. Data Transfer and Retrieval

The Contractor must provide the capability including tools and services that allow Canada to:

(a) Extract all online, nearline, and offline Canada's Data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

(b) Securely transfer all Canada's Data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/governmentinformation-resources/guidelines/Pages/guidelines-file-formats-transferring-informationresources-enduring-value.aspx).

12. Data Disposition and Returning Records to Canada

(1) The Contractor must securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Canada's Data and ensure that previously stored data cannot be addressed by others customers after it is released. This includes all copies of Canada's Data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following:

(i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

(2) The Contractor must provide Canada with confirmation that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once Canada discontinues its use of the Cloud Services.

13. Cryptographic Protection

The Contractor must:

(a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods;

(b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111);

(c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/groupgroupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and

(d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.

14. Key Management

The Contractor must ensure that a key management service can be leveraged and provides capabilities, including but not limited to:

(a) Creation/generation and deletion of encryption keys by the GC;

(b) Definition and application of specific policies that control how keys can be used;

(c) Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;

(d) Ability to audit all events related to key management services, including Contractor access for Canada's review;

(e) Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;

(f) Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and

(g) Ability to delegate key use privileges for use by the Cloud Services used for the GCmanaged services.

15. Endpoint Protection

The Contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.

16. Secure Development

The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

17. Identity and Access Management

(1) The Contractor must have the ability for Canada to support secure access to Cloud Services including ability to configure:

(a) multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;

(b) Role-based access;

(c) Access controls on objects in storage; and

(d) Granular authorization policies to allow or limit access.

(2) The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

18. Federation

(1) The Contractor must have the ability for Canada to support federated identity integration including:

(a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0, or subsequent versions, where the End User credentials and authentication to cloud services are under the sole control of Canada; and

(b) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding Cloud Service user account(s).

19. Privileged Access Management

(1) The Contractor must:

(a) Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;

(b) Restrict and minimize access to the Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;

(c) Enforce and audit authorizations for access to the Cloud Services and Canada's Data;

(d) Constrain all access to service interfaces that host Canada's Data to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);

(e) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent

versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(f) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user- authentication-guidance-information-technology-systems-itsp30031-v3);

(g) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(h) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Canada's Data;

(i) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

(j) Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and Canada's Data;

(k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Cloud Services and Contractor Infrastructure;

(l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and

(m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring privileged access of the Cloud Services.

20. Remote Management

(1) The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that are used to host GC services and take reasonable measures to:

(a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(b) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 13 (Cryptographic Protection);

(c) Route all remote access through controlled, monitored, and audited access control points;

(d) Expeditiously disconnect or disable unauthorized remote management or remote access connections;

(e) Authorize remote execution of privileged commands and remote access to security-relevant information.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Services.

21. Network and Communications Security

The Contractor must:

(a) Enforce secure connections to the Cloud Services, including providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;

(b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);

(c) Use correctly configured certificates within the TLS connections in accordance with CSE guidance.

(d) Provide the ability for Canada to implement network access controls and security rules that allow or deny network traffic to Canada resources.

22. Logging and Auditing

(1) The Contractor must implement log generation and management practices and controls for all Cloud Service components that store or process Canada's Data, and that conform with industry standards and best practices, such as those found in NIST 800-92 (Guide to

Computer Security Log Management), or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented log generation and management practices and controls.

(2) The Contractor must provide the ability for Canada to export security event logs using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.), for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

(3) The Contractor must enable Canada to centrally review and analyze audit records from multiple components from the Cloud Services consumed by the customer. This includes providing APIs that provide the ability to inspect and interrogate data at rest in SaaS applications including assessing events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access stored in SaaS application logs.

23. Continuous Monitoring

(1) The Contractor must continually manage, monitor, and maintain the security posture of Contractor Infrastructure and Service Locations hosting Canada's Data throughout the contract, and ensure that the Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(a) Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or Canada's Data;

(b) Undertake best efforts to prevent attacks through security measures such as denial of service protections;

(c) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

(d) Identify unauthorized use and access of any Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Cloud Service;

(e) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(f) Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and

(g) Where required, take proactive countermeasures, including taking both preemptive and responsive actions, to mitigate threats.

(2) The Contractor's Cloud Services must allow for GC application data of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

24. Security Incident Management

(1) The Contractor Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

(a) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/accessinformation-privacy/security-identity-management/government-canada-cybersecurity-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

(b) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the information security incidents that the Contractor will report to Canada; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents; and (vi) any remedies that apply if certain information security occur.

(c) Ability for the Contractor to support Canada's investigative efforts for any compromise of the users or data in the service that is identified.

(d) Allows only designated representatives of Customer (e.g. SSC Security Operations Center) authorized by the Technical Authority:

(i) to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
(ii) the ability for Customer to track the status of a reported information security event.

(e) Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and includes forensic procedures and safeguards for the maintenance of a chain of custody;

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's Security Incident Response Process.

(3) The Contractor must:

(a) Work with Canada's Security Operations Center(s) (e.g. CCCS, Departmental SOC) on Security Incident containment, eradication and recovery in accordance with the Security Incident Response process.

(b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and

(c) Track, or enable Canada to track, disclosure of Canada's Data, including what data has been disclosed, to whom, and at what time.

(3) Canada may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor agrees to provide assistance to the GC on a best effort basis.

25. Security Incident Response

(1) The Contractor must alert and promptly notify Canada (via phone and/or email) of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security malfunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 72 hours, and within the Contractor's service level commitments.

(2) If the Contractor becomes aware of any compromise, breach and determines a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

26. Information Spillage

(1) The Contractor must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Contractor's Information Spillage process must include, at a minimum:

(a) A process for identifying the specific data elements that is involved in a System's contamination;

(b) A process to isolate and eradicate a contaminated System; and

(c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's Information Spillage Response Process.

27. Security Testing and Validation

(1) The Contractor must have a process that allows Canada to conduct a non-disruptive and non-destructive Vulnerability Scan or Penetration Test of Canada's portion of the Cloud Service components within the Contractor environment.

(2) The Contractor must provide the ability to enable a self-service security health check or scoring tool that enables the measurement of the security posture of the Cloud Services configured by Canada.

28. Personnel Security Screening

(1) The Contractor must ensure that security measures are implemented to grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed.

(2) The Contractor screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

(3) Upon request of Canada, the Contractor must provide a document that describes the Contractor's personnel security screening process. The process must provide, at a minimum:

(a) A description of the employee and Sub-processor positions that require access to Customer Data or have the ability to affect the confidentiality, integrity or availability of the Cloud Services;

(b) A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

(c) A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing

basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;

(d) A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;

(e) The approach to detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of Cloud Services hosting Canada's data.

29. Physical (Data Centre / Facilities) Security

(1) The Contractor must ensure that physical security measures are implemented to protect the IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). The security measures required under this include, at a minimum:

(a) Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and Canada's Data within the prescribed service level commitments;

(b) Proper handling of IT Media;

(c) Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;

(d) Controlled access to information system output devices to prevent unauthorized access to Canada's Data;

(e) Limiting physical access to Canada's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

(f) Escorting visitors and monitoring visitor activity;

(g) Enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and

(h) Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting Canada's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's physical security measures.

(3) If any physical security measures is to change in a way that materially degrades the physical security, the Contractor must inform Canada.

30. Supply Chain Risk Management

(1) The Contractor must ensure that safeguards are implemented to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain.

(2) The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management Plan that is aligned with one of the following best practices:

(i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);

(ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or

(iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

(3) Within 90 days of contract award, the Contractor must:

(a) Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime

OR

(b) Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

(4) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

31. Sub-processors

(1) The Contractor must provide a list of Sub-processors that could be used to perform any part of the Work in providing Canada with the Service. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Work that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Work.

(2) The Contractor must provide a list of Sub-processors within ten days of the effective date of the Contract. The Supplier must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Customer Data or Personal Data. The Supplier must assist Canada with verification of sub-processors within 10 working days.

32. Industrial Security Program – Security Requirement for Canadian Suppliers

(1) The Contractor must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Industrial Organization Security Services Directorate (OSS), **Public Services and Procurement Canada (PSPC).**

(2) The Contractor personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required by the security guide, granted or approved by the OSS/PSPC.

(3) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED B including an IT Link at the level of PROTECTED B.

(4) The Contractor/Offeror must comply with the provisions of the:

(a) Security Requirements Check List and security guide (if applicable).

(b) Industrial Security Manual (Latest Edition);

(c) OSS website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src

NOTE: There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

33. Industrial Security Program – Security Requirements for Foreign Suppliers

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Services and Procurement Canada (PSPC), administered by International Industrial Security Directorate (IISD), PSPC. The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada for the Cloud Services described in the Cloud Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

(1) The **Contractor/Subcontractor** certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(2) The Foreign recipient **Contractor/Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor/Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA.

(3) The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract**, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:

(a) Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

(b) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's/Subcontractor's** Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

(c) The **Contractor/Subcontractor** must not grant access to **CANADA PROTECTED B** information/assets, except to personnel who have a need-to- know for the performance of the **contract** and have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures agreed to by Canada.

(d) **CANADA PROTECTED** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor /Subcontractor**, must:

i. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract**, without the prior written consent of Canada. Such consent must be sought from the Canadian DSA in collaboration with the Contracting Authority; and

ii. not be used for any purpose other than for the performance of the **contract** without the prior written approval Canada. This approval must be obtained by contacting the Contracting Authority (in collaboration with the Canadian DSA).

(4) The Foreign recipient **Contractor /Subcontractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/ Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.

(5) The Foreign recipient **Contractor /Subcontractor** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

(6) The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

(7) The Foreign recipient **Contractor/Subcontractor** must comply with the provisions of the Security Requirements Check List.

(8) Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Cloud Services to electronically access, process, produce, transmit or store **CANADA PROTECTED** data related to the Cloud Services in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.