Annex B – Schedule 2 - Privacy Obligations for Tier 2 (up to and including Protected B)

Note to Contracting Authority: All clauses apply to Workloads (Unclassified/ProA/ProB) and Delivery models (IaaS/PaaS/SaaS) unless stated otherwise

1. General

1.1 *Purpose*

The purpose of this Schedule is to set forth the privacy obligations of the Contractor relating to the use, collection, processing, transmission, storage or disposal of Canada's Data containing Personal Information (PI). Any Personal Information which is stored on Contractor systems or the Contractor is required to handle (collect, retain, use, disclose and dispose) must be safeguarded at all times by implementing administrative, physical and technical safeguards that are necessary to ensure the PI is protected commensurate to the level of injury that could arise if a privacy breach was to occur and in accordance with the Contractor Data Processing Agreement, this Schedule, and the Contractor's Specific Privacy Measures (collectively, the "**Privacy Obligations**").

1.2 *Flow-Down of Privacy Obligations*

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

1.3 *Change Management*

[Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model]

The Contractor must, throughout the Contract, take all steps required to update and maintain the Privacy Obligations as needed to comply with the security practices of industry standards.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse affect to the Cloud Service offerings in this Contract, including technological, administrative, or other types of changes or improvements that are made, and that could impact the current collection, use, disclosure and or disposal of data containing personal information. 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) All Canada's Data containing personal information are subject to these Privacy Obligations.

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

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

3. Data Ownership

(1) Canada will at all time remain the controller of the Personal Information (PI) processed by the Contractor under the Contract. Canada is responsible for compliance with Canada's privacy obligations as a controller under applicable data protection law, in particular for justification of any transmission of PI to the Contractor (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under applicable data protection law), and for Canada's decisions and actions concerning the processing of such personal data.

(2) The Contractor is and will at all times remain a processor with regard to the data containing PI provided by Canada to the Contractor under the Contract. The Contractor is responsible for compliance with its obligations under this it's Contractor Data Processing Agreement and for compliance with its obligations as a processor under applicable privacy law (i.e. Personal Information Protection and Electronic Documents Act (PIPEDA).

(3) The Contractor must not use or otherwise process Canada's Data containing PI or derive information from it for any data sharing, advertising or similar commercial purposes. As between the parties, Canada retains all right, title and interest in and to Customer Data. The Contractor acquires no rights in Customer Data, other than the rights Customer grants to the Contractor to provide the Cloud Services to Customer.

(4) All data that is stored, hosted or processed on behalf of Canada remains the property of Canada.

4. Privacy Requests

(1) Canada and the Contractor must establish a mutually agreeable process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).

(2) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] Within 30 calendar days of Contract award, the Contractor must provide a document that describes how the Contractor will support Canada in handling Access Requests, including how it will acknowledge the receipt of an Access Request, and how it will provide the requested information.

5. Third-Party Assurance: Certifications

(1) The Contractor must ensure that in respect of any personal information including Canada's Data that it may host, store or process, on Contractor Infrastructure (including any Iaas, PaaS or SaaS Service provided to Canada) and Service Locations are secured appropriate privacy and security measures that comply with the requirements set forth the Contractor's privacy practices and policies.

(2) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications 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 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Certification achieved by an accredited certification body.

(3) Each certification provided must:

[Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model]

(i) identify the legal business name of the Contractor or applicable Sub-processor;

[Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model]

(ii) identify the Contractor's or Sub-processor's certification date and the status of that certification;

[Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model]

(iii) identify the services included within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] 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) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] The Contractor is expected to maintain its certification of ISO 27018 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. Privacy Compliance

(1) The Contractor must demonstrate through third party assessment reports and audit reports that it:

(a) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] Restricts creating, collecting, receiving, managing, accessing, using, retaining, sending, disclosing and disposing of Personal Information to only that which is necessary to perform the Cloud Services and;

(b) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] Has implemented updated security processes and controls such as access management controls, human resource security, cryptography and physical, operational and communications security that preserve the integrity, confidentiality and accuracy of all information and data and metadata, irrespective of format.

7. Auditing Compliance

(1) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] In the event Canada needs to conduct security and privacy audits, inspections and/or review any additional information (e.g., documentation, data flows, data protection description, data architecture and security descriptions), both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(2) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] The Contractor must conduct the privacy and security audits of the computers, computing environment and physical data centers that it uses in processing Canada's Data containing PI 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 qualified, independent, third party security auditors that (i) is qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conforms to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(3) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] 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.

(4) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] Upon request of Canada, additional supplementary evidence from the Contractor, including system security and privacy plans, designs, or architecture documents that provide a comprehensive system description including all the data elements containing PI, 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.

8. Privacy by Design

The Contractor must demonstrate that it implements privacy by design as part of its software development lifecycle, and in accordance with Schedule 1 – Security Obligations, Section 16 (Secure Development).

9. Privacy Officer

(1) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] The Contractor must, within 10 days of the effective date of this Contract, provide Canada with information that identifies an individual as a Privacy Officer to act as Contractor's representative for all matters related to the Personal Information and the Records. The Contractor must provide that person's name and contact information including the, individual's business title, email address and phone number.

10. Assist in Delivery of Canada's Privacy Impact Assessment

(1) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] The Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308), by assisting the Canada with the supporting documentation including a foundational PIA for Canada provided by the Contractor. The Contractor agrees to provide this support within five to ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

11. Privacy Breach

(1) The Contractor must promptly evaluate and respond to incidents that create suspicion of or indicate unauthorized access to or processing of Personal Information ("**Incident**"). To the extent the

Contractor becomes aware of and determines that an Incident qualifies as a breach of privacy leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed on the Contractor's systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such Personal Information ("Personal Information Breach"), the Contractor will inform Canada of such Personal Information Breach without undue delay, and in accordance with Schedule 1 – Security Obligations, Section 26

(2) The Contractor must:

(a) [Only required for Protected B workloads & IaaS/PaaS/SaaS Delivery Model] 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; and

(b) Tracks, or enables Canada to track, disclosures of Canada's Data, including what data has been disclosed, to whom, and at what time.

12. Personal Information

The following sub-sections applies to situations where the Contractor confirms that it has access, care, and control of Canada's data.

12.1 Ownership of Personal Information and Records

(1) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] To perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Sub- processor/Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor/Sub-processor/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

12.2 Use of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Cloud Services in accordance with the **contract**.

12.3 Collection of Personal Information

(1) If the foreign recipient **Contractor/Sub-processor/Subcontractor** must collect Personal Information from a third party to perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** must only collect Personal Information that is required to perform the Cloud Services. The foreign recipient **Contractor/Subprocessor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Sub-processor/Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:

(a) that the Personal Information is being collected on behalf of, and will be provided to, Canada;

(b) the ways the Personal Information will be used;

(c) that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;

(d) the consequences, if any, of refusing to provide the information;

(e) that the individual has a right to access and correct his or her own Personal Information; and

(f) that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor/Sub-processor/Subcontractor** .

(2) The foreign recipient **Contractor/Sub-processor/Subcontractor** and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

(3) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] If requested by the Contracting Authority, the foreign recipient **Contractor/Subprocessor/Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor/Sub-processor/Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

(4) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Sub-processor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor/Sub-processor/Subcontractor** must ask the Contracting Security Authority for instructions.

12.4 Maintaining the Accuracy, Privacy, and Integrity of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor/Sub-processor/Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Subprocessor/Subcontractor** must:

(a) not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

(b) segregate all Records from the foreign recipient **Contractor's/Subprocessor's/Subcontractor's** own information and records;

(c) restrict access to the Personal Information and the Records to people who require access to perform the Cloud Services (for example, by using passwords or biometric access controls);

(d) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] provide training to anyone to whom the foreign recipient **Contractor/Subprocessor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the

Cloud Services. The foreign recipient **Contractor/Sub-processor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor/Subprocessor/Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;

(e) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor/Sub-processor/Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

(f) keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

(g) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor/Sub-processor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Sub-processsor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

(h) keep a record of the date and source of the last update to each Record;

(i) maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor/Sub-processor/Subcontractor** and Canada at any time; and

(j) secure and control access to any hard copy Records.

12.5 Safeguarding Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality, in accordance with the security measures outlined in Schedule 1 – Security Obligations.

12.6 Statutory Obligations

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, R.S.C., 1985, c. P-21, *Access to Information Act*, R.S.C., 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The

foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to comply with the requirements established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

(2) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that its obligations under the **contract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient **Contractor/Sub-processor/Subcontractor** believes that any obligations in the **contract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract** and the specific obligation under the law with which the foreign recipient **Contractor/Subprocessor/Subcontractor** believes it conflicts.

12.7 Legal Requirement to Disclose Personal Information

(1) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] If the Contractor receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the processing of Personal Information ("Disclosure Request"), it will promptly pass on such Disclosure Request to Canada without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

(2) [Only required for Protected A & B workloads & IaaS/PaaS/SaaS Delivery Model] At Canada's request, the Contractor will provide Canada with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for Canada to respond to the Disclosure Request in a timely manner.

12.8 Complaints

Canada and the foreign recipient **Contractor/Sub-processor/Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

12.9 Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.