**Information Sharing Agreement (ISA)**

|  |
| --- |
| **DATE: (month/day/year)** |

**BETWEEN:**

**Insert Name of First Party**

**(“Public Body”)**

|  |  |
| --- | --- |
| Agreement Administrator: |  |
|  | Administrator Name |
|  | Ph.: |
|  | Fax: |
|  | Email:  |

**AND:**

**Insert Name of Second Party**

**(“Party X”)**

|  |  |
| --- | --- |
| Agreement Administrator: |  |
|  | Administrator Name |
|  | Ph.: |
|  | Fax: |
|  | Email: |

 **(Collectively referred to as “the parties”)**

**Note:** Add other parties as required.

**1.0 Purpose**

**1.1** This Information Sharing Agreement (ISA) will provide for the disclosure of personal information from **<Public Body>** to **<Party X>** for the purpose(s) of:

* **<List purpose(s) for exchanging this information, including the program, service and/or project that is requesting the information.>**
* **<Indicate why the information needs to be shared – Can the work be done without it? Provide a reason for the agreement.>**

**2.0 Authority to Collect, Indirectly Collect, Use and Disclose Personal Information**

**2.1 <public body>** is authorized to collect the information identified in this ISA under:

**<cite the section(s) of the Access to Information and Protection of Privacy Act, 2015 (the Act) that allows for the original collection of the information being shared. If you are collecting personal information from someone other than the individual the information is about, also cite the authority for indirect collection. Note: If authorized in accordance with another Act, ensure the section of that legislation that authorizes the collection is cited as well.>**

**2.2 <Public Body>** is authorized to use the information identified in this ISA under:

**<cite the section(s) of the Act that allows for any uses of information relevant to this disclosure. Note: If authorized in accordance with another Act, ensure the section of that legislation that authorizes the use is cited as well.>**

**2.3** Similarly, **<Public Body>** is authorized to disclose the information outlined in this ISA to **<Party X>**for the above-stated purposes under:

**<cite the section(s) of the Act that allows for this disclosure. Note: If authorized in accordance with another Act, ensure the section of that legislation that authorizes the disclosure is cited as well.>**

**2.4** The **<Public Body>** has ensured its confidentiality notice on methods of collection reflect the uses and disclosures possible through this ISA.

**2.5** This ISA, including the appended schedules, forms the entire agreement between the parties. There are no understandings, representations or warranties of any kind except as expressly set forth herein.

**3.0 Information to be Exchanged and Mechanism for Exchange**

**3.1** **<Public Body>** will provide **<Party X>** with the personal information listed in Schedule “A”, for those purposes identified in Schedule “A” and in the mutually agreed format set out in Schedule “B”. Only the minimum information needed to achieve each listed purpose may be shared.

**3.2** The information will be handled, transferred and stored in accordance with the safeguards set out in Schedule “C”.

**4.0 Confidentiality, Use and Disclosure**

**4.1** The parties agree that the collection, use and disclosure of information covered by this ISA will be limited to the purposes outlined in this ISA.

**4.2** The parties agree that access to information covered by this ISA will be:

(a) Limited to only those employees, agents or contractors who require access for the purposes listed in Schedule “A” and will only be used or disclosed for the purposes listed in Schedule “A”.

(b) In addition, both parties agree that they will limit access to this information to the minimum amount of personal information required to achieve the intended purpose.

**4.3 <Party X>** will maintain, respect and protect the information received under this ISA, and will not use or disclose it to anyone for any purpose other than for those purposes specifically mentioned in Schedule “A”.

**4.4** Through this ISA, **<Party X>** commits to the process for employees to gain access and to have access removed as set out in **Schedule “D”**.

**5.0 Information Management and Technology**

**5.1** The Information Management (IM) arrangements below are intended to ensure the confidentiality and, integrity of personal information covered under this ISA and are intended to safeguard the personal information against accidental or unauthorized access, disclosure, use, modification and deletion.

**5.2** In order to ensure the confidentiality and integrity of the personal information exchanged in this ISA, and to safeguard the personal information against accidental or unauthorized access, disclosure, use, modification, retention or destruction, all parties agree that the information shall be collected, used, disclosed, administered, maintained, retained, destroyed or disposed of in accordance with the:

1. **Access to Information and Protection of Privacy Act, 2015**SNL2015 CHAPTER A-1.2and Regulations <http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm>
2. **Rooms Act***,* SNL 2005 c R-15.1 <http://assembly.nl.ca/Legislation/sr/statutes/r15-1.htm>; and
3. **Management of Information Act**, SNL 2005 CHAPTER M-1.01 <http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>
4. Any related records management, information protection, security and retention of records legislation, regulations, policies, directives, standards and guidelines covering the administrative, technical and physical safeguarding of the personal information, including, but not limited to:
5. the “*Protocols for Government Information on Information Technology Assets of Organization*” attached hereto as Schedule “E” ; and
6. the *Remote Access Request Form* attached hereto as Schedule “F”  for completion by the **<Party X>** for each individual employee requiring access.

**<you may add other relevant legislation, policies or procedures to this list as appropriate>**

**5.3** The information disclosed to **<Party X>** will be retained, stored and transferred in accordance with the safeguards identified in Schedule “C” of this ISA.

**5.4** Throughout the term of this ISA, it is noted that custody or control of the records may vary at times.

<**Outline the various stages of the project, and indicate whether Public Body or Party X would be considered to be** **responsible for custody or control at each stage.>**

**5.5** The information will be retained and destroyed under the retention schedule set out in Schedule “G” of this ISA.

**5.6** In the event of an unauthorized access, collection, use, disclosure, deletion, destruction or disposal of the personal information identified in this ISA, **<Party X>** agrees to:

1. Immediately notify **<Public Body>**, in writing, of the unauthorized incident with full details in accordance with the privacy breach reporting form attached hereto as Schedule “H”;
2. Provide regular and comprehensive updates, in writing, as required by **<Public Body>;**
3. Immediately take all reasonable steps required in response to the unauthorized incident;
4. In consultation with **<Public Body>**, Immediately take all reasonable steps to prevent a recurrence of the unauthorized incident;
5. **<Public Body>** must at the first reasonable opportunity notify the affected individuals that their personal information has been breached as stipulated by the *Access to Information and Protection of Privacy Act, 2015* unless the head of the public body determines that section 64(7) of the Act applies; or

**<Public Body>** reserves the right to direct **<Party X>** to notify the affected individuals where **<Party X>** is a “public body” as defined under the Act.
6. **<Public Body>** must notify the Office of the Information and Privacy Commissioner of the breach as mandated under s. 64(4) of the Act. **<Public Body>** reserves the right to direct **<Party X>** to notify the Office of the Information and Privacy Commissioner where **<Party X>** is a “public body” as defined under the Act.

**5.7** If for any reason it is deemed appropriate by **<Public Body>**, including in the event of an unauthorized incident, **<Public Body>** may terminate access by the **<Party X’s>** employee(s), agent(s), contractor(s) or the **<Party X>** for a period of time up to and including no future access. The inability of an individual to complete the normal duties of their position will not preclude **<Public Body>** from terminating access.

**5.8** Each party will advise the other party of any changes in its Information Management practices and procedures that may affect the protection of personal information and obtain the other party’s consent prior to such changes.

**5.9** The parties, separately or jointly, will conduct a periodic review of Information Management practices and procedures outlined under this ISA to ensure compliance with this ISA.

**6.0 Ensuring Data Protection**

**6.1** The parties agree that they are responsible for the actions of their own employees, agents and

contractors with respect to the collection, use, disclosure, retention, and disposal of personal information in their custody or under their control, regardless if the person is or was acting within the scope of his or her employment, agency or contract.

**6.2 <Party X>** will advise **<Public Body>** of any changes to the employees, agents or contractors who access the information on behalf of **<Party X>** within 24 hours of the change in role. Upon receipt of the staff change **<insert appropriate employee**> or her/his designate will record the staff change and initiate the appropriate system access change.

**6.3 <Public Body>** reserves the right to deactivate the accounts ofemployees, agents or contractors of **<Party X>** if said employees, agents and contractors have not accessed the information in 30 days.

**6.4** The Parties will not store “personal information”, as defined under the Act, from the **<system>** on any device or service outside Canada.

**6.5 <Party X>** must notify **<Public Body>** where the information is stored.

**6.6** In order to monitor compliance with the Act, **<Party X>** is responsible for preparing activity

 reports every **<identify timeframe>**, and provide these to the **<Public Body**>. This is to be completed

 to ensure that information is not being accessed inappropriately. Failure to produce these reports is

 considered a breach of this ISA and may result in a termination of information sharing from the

 **<Public Body>.**

**<Note: depending on the system being used, the public body may be the party required to**

 **prepare the reports, with <Party X> reviewing. This statement may be modified as required.>**

**6.7** **<Party X>** agrees to ensure that all employees, agents or contractors with access to the information

received under this ISA will be provided with appropriate training related to the protection and approved use and disclosure of this information, upon initial approval, and at a minimum, annually thereafter. Records of this training will be maintained by **<Party X>** and will be made available to **<Public body>** upon request.

**7.0 Accuracy**

**7.1** **<Public Body>** will, to the best of its ability, ensure the completeness and accuracy of the information

 provided to **<Party X>** under this ISA. However, it is understood and agreed that they cannot guarantee

 its accuracy and will, therefore, not be held responsible for any damage resulting from the transmission

 or use of any information that is inaccurate or incomplete.

**7.2** **<Public Body>** and **<Party X (if it is a public body)>** agree to review any requests from individuals for correction of their personal information that may be in the custody or under the control of that party, in accordance with the Act.

**7.3** Neither **<Public Body>** or **<Party X>** will alter personal information on the request of a third party without the consent of the individual to which the information pertains.

**8.0 Amendments**

**8.0** This ISA may be modified with the written consent of designated officials from **<Public Body>** and **<Party X>.**

**9.0 Auditing Requirements**

**9.1** **<insert who is completing audits, what is to be audited and time period of audits>**

In circumstances where the entity is found to be in compliance with this ISA, and has had no breaches, **<Public Body>** reserves the right to change the audit period from **<insert>** to **<insert>**. If at any time the entity becomes noncompliant with this ISA the audit period will be adjusted at the discretion of the **<Public Body>.**

**9.2** Upon receipt of the audit report, **<Party X>** must conduct a review of the report by the **<insert date>** to ensure all inquiries relate to the purpose(s) for which access was authorized. **<Party X>** must confirm for **<Public Body>**, via email to **<insert appropriate public body employee>**, that the audit report has been reviewed and no inappropriate access has been identified. The audit report must be signed and dated by an authorized supervisor/manager of **<Party X>** and be made available to **<Public Body>** upon request.

 Users are not permitted to audit their own access to the system; audits must be conducted by a user’s supervisor.

 **<Public Body>** must be notified of a change in the audit recipient within 24 hours.

**9.3** Upon completion of the **<insert frequency>** audit, **<Party X>** must immediately notify **<Public Body>**, in writing, where it suspects an unauthorized incident may have occurred.

 Where **<Party X>** is a “public body” as defined under the Act and suspects an unauthorized incident may have occurred it must report the incident to the Office of the Information and Privacy Commissioner as mandated under the Act.

**9.4** Where **<Party X>** is a “public body” as defined under the Act, and where an unauthorized incident has occurred, **<Party X>** must notify the affected individual of the breach of their personal information as stipulated in the Act unless the head of the public body determines that sub-section 64(7) of the Act applies.

**9.5** **<Public Body>** shall have the right, from time to time, to audit **<Party X’s>** records related to obligations under this ISA.

**9.6** The audit will be conducted during the normal business hours of **<Party X>** upon 10 days advance notice.

**9.7** **<Public Body>** shall have the right to engage third party representatives to perform the audit.

**9.8** **<Party X>** will fully cooperate with **<Public Body>** in facilitating the conduct of an audit, including providing such access, documentation, information, copies of documentation and information and assistance as **<Public Body>** may reasonably require for the purpose of an audit.

**9.9** **<Party X>** shall, at its sole cost, immediately correct any breaches of this ISA identified through an audit. **<Party X>** shall notify **<Public Body>** in writing as soon as such breaches have been corrected.

**9.10** All costs incurred by **<Party X>** in connection with an audit shall remain solely the responsibility of **<Party X>.**

**9.11** All costs incurred by **<Public Body>** in connection with the audit shall remain solely the responsibility of **<Public Body>**.

**9.12** **<Public Body>** may require **<Party X>** to meet with **<Public Body>** officials to review the results of an audit. Such meetings shall be held at such times and places as **<Public Body>** and **<Party X>** may mutually agree upon.

**9.13** Prior to the expiration of this ISA and before a new ISA will be signed **<Party X>** will complete a mini-audit for each year the ISA has been in place which will include a review of audit information for access management and a review of employee training records, which mini-audit shall be supplied to **<Public Body>.**

**10.0 Expiry**

**10.1** This ISA will expire on **<date>** unless earlier terminated in accordance with this ISA.

**10.2** Should this ISA be subject to renewal, a review of **<Party X>**‘s activities is required before the

 renewal is approved, including access logs and training details.

**10.3** Clauses 4, 5, 6, and 9 shall survive the expiration or termination of this ISA.

**11.0 Coordinating Office**

**12.1** If an issue arises as to whether the provisions of the Act apply to **<Party X>** identified in the ISA, the parties may consult with:

**<Insert an appropriate contact person and details>**

**12.0 Notices**

**12.1** All notices, requests, updates and other communications required under this ISA shall be in writing. The addresses for service are as follows:

**For the <Public Body>:**

**<insert an appropriate contact person and details>**

**For the <Party X>**

**<insert an appropriate contact person and details>**

Notices, requests, updates or documents shall be deemed to have been received by the addressee as follows:

* + 1. As of the date on which they are delivered where delivery is by a party or by messenger or special courier service;
		2. As of the date on which they are sent where delivery is by electronic communication; and
		3. Six (6) days after delivery to Canada Post Corporation where the postal service is used.

**13.0 Sign-Off**

**13.1** Agreed to on behalf of **<Public Body>:**

**<Name of Authorized Individual>**

**<Title of Authorized Individual>**

**<Address>**

**<Telephone Number>**

**<Fax Number>**

**<Email>**

**13.2** Agreed to on behalf of **<Party X>:**

**<Name of Authorized Individual>**

**<Title of Authorized Individual>**

**<Address>**

**<Telephone Number>**

**<Fax Number>**

**<Email>**

**13.3** Date of Agreement: **<Insert date>**

**13.4** Signatures



On Behalf of **<Public Body>**



On Behalf of **<Party X>**

**Schedule “A”**

|  |  |  |
| --- | --- | --- |
| **Personal Information being Disclosed** | **Who it will be Used by (include name or position title)** | **Purpose of Use/Why this Information is Needed** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Schedule “B”**

|  |  |  |
| --- | --- | --- |
| **Personal Information being Disclosed** | **Format of disclosure\*** | **Manner of disclosure e.g. email, fax, etc.** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**\*If using a standardized form to share information, you should attach it to this scheduleSchedule “C”**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Technical Safeguards** | **Physical Safeguards** | **Administrative Safeguards** |
| **Transfer** | **<List>** | **<List>** | **<List>** |
| **Storage/Retention** | **<List>** | **<List>** | **<List>** |

**Schedule “D”**

**<Outline the process to be used to provide an employee with access to personal information and the process to remove that access>Schedule “E”**

**<insert the most up-to-date version available of the “*Protocols for Government Information on Information Technology Assets of Organization*”, available from the Office of the Chief Information Officer>**

**Schedule “F”**

**<insert the most recent version of the *Remote Access Request Form*, available from the Office of the Chief Information Officer>**

**Schedule “G”**

**<Insert Retention Schedule>**

**Schedule “H”**

**<insert most recent version of the Privacy Breach Reporting Form, available from the Office of the Information and Privacy Commissioner>**