

**CONTRACT FOR ACCESS TO A RESEARCH FILE WITH  
REMOTE ACCESS MICRODATA FILE**

**BETWEEN: INSTITUT DE LA STATISTIQUE DU QUÉBEC**, a body legally instituted under the *Act respecting the Institut de la statistique du Québec* (CQLR, chapter I-13.011), having its head office at 200, chemin Sainte-Foy, 5th floor, Québec QC G1R 5T4, acting through Mr. Simon Bergeron, Chief Statistician, duly authorized for the purposes hereof;

hereinafter “the Institut”

**AND MS./MR.** First name Last name, title, department, organization, address;

hereinafter “the Researcher”

**AND PUBLIC BODY XXXX**, having its head office at address, XXX QC postal code, represented by Ms./Mr. (name of signatory), (function of signatory), duly authorized for the purposes hereof;

hereinafter “the Public Body”

The Institut, the Researcher and the Public Body are hereinafter referred to individually or collectively as “the Party(ies)”.

**WHEREAS** under section 2.1 of the *Act respecting the Institut de la statistique du Québec* (hereinafter “*Act respecting the Institut*”), the Institut’s mission is to ensure the communication, for research purposes, of information held by public bodies to researchers linked to a public body as defined in section 2.2 of the *Act respecting the Institut*;

**WHEREAS** under the first paragraph of section 13.1 of the *Act respecting the Institut*, the government may designate information held by a public body so that it may, in accordance with this Act, be communicated for research purposes to researchers linked to a public body;

**WHEREAS** government orders in effect under the second paragraph of section 13.1 of the *Act respecting the Institut* allows the Institut to communicate designated information (hereinafter “Designated Information”) when researchers linked to a public body request it;

**WHEREAS** the principal researcher for the Public Body, hereinafter “the Researcher”, is working on the research project “XXX”, hereinafter “the Research Project” as defined in Schedule A hereto;

**WHEREAS** a research file without identifying information (“Research File”) is created for the Research Project and access to this Research File must take place in accordance with the terms and conditions of access in force at the Institut;

**WHEREAS** the Researcher is requesting access to the Research File for the purpose of carrying out the Research Project and agrees to be considered, for this purpose, a person whose services are retained by the Institut, but without remuneration, and to be governed accordingly by the obligation of discretion provided for in section 25 of the *Act respecting the Institut* and will sign a confidentiality agreement to that effect (Schedule C1);

**WHEREAS** a person referred to in section 25 of the *Act respecting the Institut* may not, under section 30 of that Act, be compelled to reveal what was disclosed to them or what they learned in the exercise of the functions described in paragraphs 1 and 5 of section 5 of that Act or to produce a document prepared or obtained in the exercise of those functions before a court or before a body or a person exercising an adjudicative function.

**NOW THEREFORE, THE PARTIES AGREE AS FOLLOWS:**

**1. PURPOSE**

The purpose of this contract is to establish the terms and conditions of access to the Research File created for the Research Project defined in Schedule A. More specifically, its aim is to set out the conditions and obligations of the Researcher and the body he or she is linked to, i.e., the Public Body, as well as those of the Institut regarding the use of and access to the Research File in a form adapted for remote access called “Remote Access Microdata File”, hereinafter “RAMF”, as well as the use of intermediate results tables, hereinafter “Intermediate Results”, that can be accessed remotely by the Researcher.

**2. OBLIGATIONS OF THE INSTITUT**

2.1 The Institut undertakes to make the following available to the Researcher and the persons authorized in Schedule B, hereinafter “Authorized Persons”, for the Research Project:

2.1.1 The Research File at one of its Research Data Access Centres (CADRISQ) using the equipment provided and/or designated by the Institut;

2.1.2 The RAMF via secure remote access, which remains within the Institut’s technological infrastructure at all times in order to respect the protection of the confidential information it contains, and in accordance with the requirements set out in Schedule D;

2.1.3 Intermediate Results via secure remote access, which remain within the Institut’s technological infrastructure at all times in accordance with the requirements set out in Schedule D;

- 2.1.4 The basic information and documentation needed to use the Research File, as well as a guide explaining the confidentiality and security rules to be respected;
  - 2.1.5 A work schedule that balances the Researcher's needs with the Institut's resources;
  - 2.1.6 A remote work environment available at all times except during maintenance periods. Malfunctions will be corrected on business days between 8:30 a.m. and 4:30 p.m.;
  - 2.1.7 Statistical software such as RStudio, SAS EnterpriseGuide, SPSS or Stata, to be specified by the Researcher and the Authorized Persons, in the version available at the Institut, as well as the Office suite (Word, Excel and PowerPoint). Any other software is installed at the Researcher's expense.
- 2.2 The Institut undertakes to respond to all technical support requests in a timely manner.
  - 2.3 The Institut undertakes to respond in a timely manner to requests for confidentiality checks on any reasonable amount of results produced by the Researcher and/or the Authorized Persons that are to be retrieved from the secure environment.
  - 2.4 If the Researcher requests access to RAMF and Intermediate Results from a location outside the province of Québec, the Institut will assess this request and may authorize it if the standards in effect at the Institut are met.
  - 2.5 The Institut undertakes to notify without delay the Commission d'accès à l'information (CAI) and the public body that communicated the Designated Information integrated into the Research File and RAMF in the event of non-compliance with any condition set forth in this contract, of any breach of the protective measures set forth in this contract or of any event likely to compromise the confidentiality of the Research File and RAMF.

### **3. OBLIGATIONS OF THE RESEARCHER**

The Researcher undertakes to:

- 3.1 Provide any necessary or useful information, approval or instruction to enable the Institut to fulfill its obligations without undue delay;
- 3.2 Protect the confidentiality of the information contained in the Research File, in the RAMF, and in Intermediate Results, and more specifically to:
  - 3.2.1 Provide the list of Authorized Persons who will have access to the Research File, RAMF, and Intermediate Results and notify the Institut as soon as possible of any changes to this list and the effective date of such update. The Researcher must therefore inform the Institut as soon as an Authorized Person withdraws

from the project or no longer needs to have access to the data covered by this contract so as to remove this person's authorization to access the data. The same is true when the Researcher wants to add a new person to the list of Authorized Persons;

- 3.2.2 Make sure that the Authorized Persons who access the RAMF and Intermediate Results are located in the province of Québec, or request the Institut's authorization if they reside outside the province of Québec or access these from outside the province of Québec;
  - 3.2.3 Have all Authorized Persons sign the confidentiality agreement form provided in Schedule C2, inform them of the possible sanctions for any breach of confidentiality, and send the forms to the Institut as soon as possible;
  - 3.2.4 Comply with the security and confidentiality requirements for secure remote access set forth in Schedule D hereto, and, where applicable, have any Authorized Person do likewise;
  - 3.2.5 Have an Institut representative conduct a check on any results before moving them by any means whatsoever outside the Institut's technological infrastructure and provide the Institut with the information needed for that purpose.
- 3.3 Comply with and have any Authorized Person comply with the following rules:
- 3.3.1 Use the Research File, RAMF and Intermediate Results only for the purpose of the Research Project;
  - 3.3.2 Make no attempt to re-identify individuals;
  - 3.3.3 Not compare, link or match individuals from the Research File, RAMF, Intermediate Results or a file derived from another file;
  - 3.3.4 Not import any unauthorized files by any means whatsoever into the Institut's work environment;
  - 3.3.5 Not copy the Research File, RAMF, or Intermediate Results to any medium or move them by any means whatsoever outside the Institut's work environment;
  - 3.3.6 Not use the technological environment provided by the Institut to access a file not covered by this contract or to copy or move such a file;

- 3.3.7 Not provide access to the Research File, RAMF, Intermediate Results, or any derivative files to any unauthorized person;
  - 3.3.8 Have an Institut employee conduct a risk-of-disclosure check on any results to be exported from the Institut's technological environment and provide this Institut employee with all information needed for that purpose, according to the instructions provided by the Institut;
  - 3.3.9 Not disseminate or publish any results that could link information, even indirectly, to a person or any other identifiable unit, such as a company, institution, school or other;
  - 3.3.10 Comply with all guidelines and instructions that will be given by the Institut representative regarding the use of data, particularly in terms of confidentiality and physical and computer security.
- 3.4 Allow the Institut to conduct, upon request, any check it deems necessary to ensure compliance with the confidentiality and security rules set forth in Schedules D and E hereto;
  - 3.5 Notify the Institut without delay in the event of non-compliance with any condition set forth in this contract, of any breach of the protective measures set forth in this contract or of any event likely to compromise the confidentiality of the Research File, RAMF, and Intermediate Results;
  - 3.6 Notify the Institut when a court, body or person exercising adjudicative functions summons the production of documents related to the Research File or RAMF following their use or issues an order to access the Research File or RAMF. Pursuant to section 30 of the *Act respecting the Institut*, a person referred to in section 25 of this Act may not be compelled to reveal what was disclosed to them or what they learned in the exercise of the functions described in paragraph 1 of section 5;
  - 3.7 Notify the Institut prior to any media contact regarding the Research File or RAMF following their use;
  - 3.8 Send information to the Institut regarding the publication of results from their research, including the title and date of publication, the name of the public body to which the researcher is linked, the name of the researcher linked to the public body, as well as the bibliographic reference and/or link, if applicable, to maintain the register of publications of research results, as required under section 13.16 of the *Act respecting the Institut*. The researcher must also make the publication(s) available upon request;
  - 3.9 Provide the Authorized Persons with a secure room whose access and security conditions are as specified in Schedule D hereto and/or ensure that they have access to such a room for remote access to the RAMF and Intermediate Results.

- 3.10 Ensure that any person acting under this contract has not been convicted of a criminal or penal offence inconsistent with their functions, including data theft, identity theft and data fraud. To this end, if the Institut has reason to believe that such an offence has occurred and in order to avoid any confidentiality incident, it may ask the person identified in Schedule B to provide a security clearance or criminal background check issued by the Public Body, while keeping the Public Body and the Researcher informed of any such procedure.

#### **4. OBLIGATIONS OF THE PUBLIC BODY**

- 4.1 The Public Body undertakes to ensure that the Researcher acting under this contract has not been convicted of a criminal or penal offence inconsistent with their functions.
- 4.2 The Public Body shall provide the Researcher with whom it has a contractual relationship with a room whose access and security conditions are as specified in Schedule D or ensure that they have access to such a room for remote access to the RAMF and Intermediate Results.
- 4.3 The Public Body vouches for the Researcher and is responsible for the latter regarding the obligations which concern him, particularly with regard to data confidentiality, physical security, and computer security.

#### **5. ACCESS TO INTERMEDIATE RESULTS AND RAMF IN A TELEWORK CONTEXT**

- 5.1 The Public Body shall authorize the Researcher to perform his or her professional duties remotely from a location other than his or her usual premises, i.e., outside the offices of the Public Body, as long as the conditions are as set forth in Schedule E hereto.
- 5.2 The Public Body is responsible for the Researcher and guarantees that he or she will abide by the terms of access and conditions attached hereto as Schedule E, since it allows the Researcher to act as a teleworker in carrying out the work to be done as part of the Research Project.
- 5.3 The Researcher undertakes to comply with the terms of access and conditions attached hereto as Schedule E regarding telework and to ensure that the Authorized Persons also comply with them.
- 5.4 The Institut shall provide the Researcher with telework access to the RAMF and Intermediate Results according to the terms set forth hereto and according to the conditions of access set forth in Schedule B and, where applicable, shall provide any Authorized Person with such access. The Institut reserves the right to remove telework access if the Researcher and Authorized Persons do not comply with the requirements or for any other reason resulting from the application of the *Act respecting the Institut*.

## 6. APPLICABLE SANCTIONS

In the event of a breach of this contract by the Researcher, the Public Body, or any Authorized Person, the following sanctions may be applied:

- 6.1 Access to the Research File, RAMF and Intermediate Results, if applicable, will be withdrawn and the Institut will refuse to enter into any further contracts of the same nature with the Researcher if the Researcher or an Authorized Person is responsible for the breach, and with the Public Body if the Public Body or the Researcher is responsible for the breach;
- 6.2 The Researcher or the Public Body will be prosecuted under the penal provisions of sections 41, 42 and 42.1 of the *Act respecting the Institut* or similar provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, chapter A-2.1) or any other law that may be invoked.

## 7. CONFIDENTIALITY

- 7.1 The Parties hereto agree to comply with applicable laws regarding information and confidentiality.
- 7.2 The Parties agree to take all protective and security measures necessary to maintain the confidentiality of information.
- 7.3 The Parties undertake not to disclose or cause to be disclosed, by any means whatsoever, any information if such disclosure would allow the information to be linked to a specific person, company, organization or association.
- 7.4 The Parties hereto undertake not to disclose or cause to be disclosed, without being duly authorized to do so, any confidential information of which they may have become aware in the performance of this contract.
- 7.5 Each Party shall inform the other Parties as soon as possible of any breach of the obligations in this confidentiality clause.

## 8. MATERIAL AND INTELLECTUAL PROPERTY

Material property

- 8.1 The Research File, RAMF, and Intermediate Results remain the sole material property of the Institut.
- 8.2 The results of the use of the Research File and RAMF for the purposes of the Research Project become the material property of the Researcher and/or the Public Body (DEPENDING ON THE CASE).

Copyright

- 8.3 The Research File and RAMF are the work of the Institut and are owned by the Institut.

- 8.4 The Researcher and/or the Public Body (DEPENDING ON THE CASE) hold the copyright on the results obtained from the use of the Research File and RAMF for the purposes of the Research Project.
- 8.5 The Institut grants the Researcher and the Public Body (DEPENDING ON THE CASE FOR THE PUBLIC BODY) a revocable, non-exclusive, non-transferable, non-sublicensable license to use and adapt the Research File and RAMF, in whole or in part, for the purposes of the Research Project, as permitted by law.
- 8.6 The Institut grants the Researcher and the Public Body (DEPENDING ON THE CASE FOR THE PUBLIC BODY) a revocable, non-exclusive, non-transferable, non-sublicensable license to use and adapt Intermediate Results, in whole or in part, without publication or dissemination, for the purposes of the Research Project, as permitted by law.
- 8.7 In the event that the license should be revoked, the Institut undertakes to explain the reason to the Public Body and to determine in good faith with the latter a solution that will not compromise the Research Project in progress.
- 8.8 This license is granted free of charge according to the Research File retention period specified in the Research Project.
- 8.9 When using this license, the Researcher and the Public Body (IF APPLICABLE) undertake to meet the following obligations and shall ensure that the Authorized Persons are informed of and bound by them:
- a) Include the following statement in references to any reproduction, adaptation, publication, dissemination or public communication of results based on the use of the Research File in the form of a table, graph or other product: “© Gouvernement du Québec, Institut de la statistique du Québec (year of publication of the Research File or RAMF)”;

IF THE RESEARCH FILE OR RAMF CONTAINS INFORMATION FROM STATISTICS CANADA, THE FOLLOWING MUST BE ADDED:

“Source: Adapted from Statistics Canada by the Institut de la statistique du Québec, product name, reference date. This does not constitute an endorsement of this product by Statistics Canada.”

- b) Specify that the Government of Québec is not responsible for the compilation or interpretation of the results produced based on the Research File or RAMF.

#### Warranties

- 8.10 The Institut warrants to the Researcher and/or the Public Body (IF APPLICABLE) that it holds all rights to grant the copyright licenses provided in this contract.

#### Exclusions

- 8.11 The licenses granted by the Institut to the Researcher or the Public Body (IF APPLICABLE) as described hereto exclude the use of the Research File and RAMF as evidence before a court, organization or individual exercising adjudicative functions, pursuant to section 30 of the *Act respecting the Institut*.

## 9. TERM

This contract shall become effective as of the date of the last signature and shall remain in effect for XXXX years from that date. It will therefore end on the XXXX anniversary of the date of last signature, unless previously terminated or unless the Parties agree in writing to extend the contract.

## 10. RETENTION AND DESTRUCTION

- 10.1 Pursuant to sections 30.2 and 30.3 of the *Act respecting the Institut*, the Institut undertakes to keep the Research File and RAMF in its secure environment for a period of XXXX years from the access end date specified for the Researcher and the Public Body.
- 10.2 The Research File and RAMF will be destroyed at the end of the retention period, as set out in clause 10.1.

## 11. AMENDMENT

To be valid, any amendment hereto must be in writing and signed by all Parties.

## 12. TERMINATION

- 12.1 Any of the Parties may terminate this contract, for any reason, by giving 30 days written notice of termination to the other Parties, with termination taking effect on the notice expiration date. The Parties may also agree on a date of termination.
- 12.2 If the Researcher and/or the Authorized Persons breach or allow any person to breach the terms of this contract, the Institut shall immediately terminate this contract by written notice to the persons concerned.

## 13. MISCELLANEOUS PROVISIONS

- 13.1 The preamble and schedules form an integral part of this contract as if recited in full. The Parties acknowledge that they have received a copy of the contract, have read it and agree to the terms and conditions set forth therein. In the event of any inconsistency or conflict between any provision contained in any part of the contract preceding the signature block and any provision in the schedules hereto, the provision contained in the part of the contract preceding the signature block shall prevail.
- 13.2 The Parties cannot be held responsible for any failure or delay of performance caused by unforeseeable circumstances beyond their control, including, without limitation, natural disasters, fires, labour disputes, wars,

epidemics, and pandemics (including the COVID-19 pandemic), if an unreasonable effort on the part of the concerned Party would be required to avoid such circumstances.

- 13.3 The Parties are independent contractors for the purposes of the Research Project. This contract does not create any employment relationship, partnership, or principal-agent relationship.
- 13.4 The provisions hereto relating to restrictions on the various schedules, confidentiality, intellectual property, penalties, and any other provisions that, by nature, are intended to survive the termination or expiration of this contract, shall survive the termination or expiration of this contract.
- 13.5 This contract, including the interpretation, execution, enforcement, validity and effects thereof are subject to the laws in force in the Province of Québec, and the laws of Canada that apply govern all the provisions hereto. The Parties submit irrevocably to the exclusive jurisdiction of the courts of the Province of Québec.
- 13.6 Any tolerance or indulgence shown by one Party to another Party, or any partial or limited exercise of a right conferred on a Party, shall not constitute a waiver of that Party's rights unless expressly waived in writing by that Party.
- 13.7 This contract may be signed in counterparts, and each counterpart may be delivered by facsimile or in PDF format. Each counterpart shall constitute an original, and when taken together, they shall constitute one and the same instrument.

#### **14. NOTICES AND CORRESPONDENCE**

- 14.1 To be valid and binding on the Parties, correspondence and notices to be given hereunder must be in writing and sent by a means that provides proof of receipt at a specific time.
- 14.2 Any correspondence or notices to be made hereunder must be addressed to the persons responsible for the administration of this contract.
- 14.3 The Parties designate the following individuals as contract administrators:

For the Institut:

First and last name

Director

Direction de la gestion des données et de l'accès pour la recherche

Institut de la statistique du Québec

200, chemin Sainte-Foy, 2nd floor

Québec QC G1R 5T4

Telephone: XXXX

Email: XXXX

For the Researcher:

First and last name  
Title  
Public body  
Address  
City (Québec) Postal code  
Telephone: XXX-XXX-XXXX, ext. XXXX  
Email: XXXX

For the Public Body:

First and last name  
Title  
Public body  
Address  
City (Québec) Postal code  
Telephone: XXX-XXX-XXXX, ext. XXXX  
Email: XXXX

- 14.4 If the contract administrator for one Party must be replaced during the term of this contract, the Parties agree to notify the other Parties and to provide a replacement as soon as possible.

Courtesy translation



SCHEDULE A

*Courtesy translation*

**SCHEDULE B<sup>1</sup>**  
**LIST OF AUTHORIZED PERSONS**  
 Access to the Research File at CADRISQ or by secure remote access (see Schedule D)

Data access conditions								
First and last name	Affiliation	CADRISQ			Remote access <sup>2</sup>		Telework access <sup>3</sup>	Outside Québec <sup>4</sup> (Access location)
		Start date	End date	Research file	RAMF	Intermediate Results tables	RAMF and/or Intermediate Results	
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<sup>1</sup> Only those individuals who need to access the research files and/or RAMF to carry out analyses or view Intermediate Results (IR) must be listed in Schedule B. IR are results from exploratory analyses. They are not intended for release and must remain in the ISQ's secure environment. Note that final results that have undergone a risk-of-disclosure analysis can be released to all outside the ISQ's environment.

<sup>2</sup> Information on the Authorized Person's remote access location (located in the associated institution) must be provided in the request form submitted to the Data Access Services.

<sup>3</sup> Information on the Authorized Person's telework access location (located in the home) must be provided in the request form submitted to the Data Access Services.

<sup>4</sup> Any Authorized Person accessing the Research File, RAMF or IR must be located in the province of Québec or must request authorization from the ISQ to access them from outside the province of Québec.

**SCHEDULE C1**  
**CONFIDENTIALITY AGREEMENT**  
**(SIGNING RESEARCHER)**

I, **NAME OF RESEARCHER**, the undersigned, in my capacity as “role”, request access to the information and files identified in the contract between the Institut and the undersigned bearing file number 40XXX-2X, for the purpose of carrying out the project “Project Title”. I agree to be considered, for this purpose, a person whose services are retained by the Institut de la statistique du Québec, but without remuneration, and to be governed by the obligation of discretion provided for in section 25 of the *Act respecting the Institut de la statistique du Québec* (CQLR, chapter I-13.011).

**WHEREAS** said section 25 of the *Act respecting the Institut* provides that:

“The Chief Statistician, assistant chief statisticians, public servants and any other person whose services are used by the Chief Statistician in the exercise of the Chief Statistician’s functions shall not disclose or cause to be disclosed, by any means whatsoever, any information obtained under this Act if disclosure would allow information to be associated with a specific person, enterprise, body or association”;

**WHEREAS** I have read Schedules D and E hereto and shall comply with the security and confidentiality requirements therein, and I understand the implication of any breach of these requirements;

**WHEREAS** I have read the details of the Research Project as set out in Schedule A hereto, I more specifically undertake to strictly adhere to the research objectives specified therein, and I understand that the Designated Information communicated as part of this contract can be used solely to meet these objectives;

**WHEREAS** if I breach the obligations set out in this contract, I may be liable to sanctions such as withdrawal of access to the Research File and Intermediate Results tables, if applicable, and/or legal proceedings under the penal provisions set out in sections 41, 42 and 42.1 of the *Act respecting the Institut*;

**WHEREAS** said sections 41, 42 and 42.1 of the *Act respecting the Institut* provide that:

“41. A person is guilty of an offence where the person:

(1) discloses, contrary to this Act and without reasonable excuse, information obtained for the purposes of this Act;

(2) makes use of information obtained in the exercise of the person’s functions to obtain undue advantage for the person or any other person;

(3) obtains or attempts to obtain, under the pretence of the exercise of the person’s functions, information that the person is not authorized to obtain;

(...)

(5) incites or encourages a person referred to in [section 25](#) to disclose, contrary to this Act, information obtained for the purposes of this Act;

(...)

42. Any person who contravenes [section 41](#) is liable to a fine of \$200 to \$1,000 and, for any subsequent offence, to a fine of \$500 to \$2,500.

42.1. On an application made by the prosecutor and submitted with the statement of offence, the judge may impose on the offender, in addition to any other penalty, a further fine not exceeding the financial benefit realized by the offender as a result of the offence, even if the maximum fine has been imposed.”

**NOW THEREFORE**, I solemnly declare that I undertake to keep secret, indefinitely, all information of which I may become aware in the course of accessing and using the information and files identified in the contract.

As a signatory, I more specifically declare that:

- I shall comply with the Institut’s confidentiality and security requirements in the course of using the information and files identified in the contract, and I undertake to read the specific instructions given by the Institut. In the event of any inconsistency or conflict between any requirements, I shall notify the Institut or my organization if notice cannot be given to the Institut, and I shall apply the most stringent instructions;
- I shall access the information and files identified in the contract only if my duties require it and circumstances justify it and solely for the purposes of the Research Project;
- I shall neither disclose nor make known any confidential information that I have learned and I undertake to keep this information confidential in perpetuity;
- I am fully aware that the Institut may use mechanisms to oversee information security and protection, and that any confidentiality incident on my part may lead to disciplinary sanctions;
- I am fully aware that the Institut has the right to review the use of the information and files identified in the contract for the authorized project for verification, control, protection, and information security purposes.

And I have signed: \_\_\_\_\_  
NAME OF RESEARCHER

<b>Swearing-in</b>
Signed before me, _____ (No. _____ ) in _____, this _____ day of _____. <div style="display: flex; justify-content: space-around; font-size: small; margin-top: 5px;"> <span>(place)</span> <span>(date)</span> <span>(month and year)</span> </div>
(Signature of commissioner for oaths or legal practitioner)

**SCHEDULE C2**  
**CONFIDENTIALITY AGREEMENT**  
**(PERSONS AUTHORIZED UNDER SCHEDULE B)**

---

I, **NAME OF AUTHORIZED PERSON**, the undersigned, in my capacity as “role”, request access to the information and files identified in the contract between the Institut and **NAME OF PRINCIPAL RESEARCHER** bearing file number 40XXX-2X, for the purpose of carrying out the project “Project Title”. I agree to be considered, for this purpose, a person whose services are retained by the Institut de la statistique du Québec, but without remuneration, and to be governed by the obligation of discretion provided for in section 25 of the *Act respecting the Institut de la statistique du Québec* (CQLR, chapter I-13.011)

**WHEREAS** said section 25 of the *Act respecting the Institut* provides that:

“The Chief Statistician, assistant chief statisticians, public servants and any other person whose services are used by the Chief Statistician in the exercise of the Chief Statistician’s functions shall not disclose or cause to be disclosed, by any means whatsoever, any information obtained under this Act if disclosure would allow information to be associated with a specific person, enterprise, body or association.”

**WHEREAS** if I breach the obligations set out in this contract, I may be liable to sanctions such as withdrawal of access to the Research File and Intermediate Results tables, if applicable, and/or legal proceedings under the penal provisions set out in sections 41, 42 and 42.1 of the *Act respecting the Institut*;

**WHEREAS** said sections 41, 42 and 42.1 of the *Act respecting the Institut* provide that:

“41. A person is guilty of an offence where the person:

- (1) discloses, contrary to this Act and without reasonable excuse, information obtained for the purposes of this Act;
- (2) makes use of information obtained in the exercise of the person’s functions to obtain undue advantage for the person or any other person;
- (3) obtains or attempts to obtain, under the pretence of the exercise of the person’s functions, information that the person is not authorized to obtain;
- (...)
- (5) incites or encourages a person referred to in [section 25](#) to disclose, contrary to this Act, information obtained for the purposes of this Act;
- (...)

42. Any person who contravenes [section 41](#) is liable to a fine of \$200 to \$1,000 and, for any subsequent offence, to a fine of \$500 to \$2,500.

42.1. On an application made by the prosecutor and submitted with the statement of offence, the judge may impose on the offender, in addition to any other penalty, a further fine not exceeding the financial benefit realized by the offender as a result of the offence, even if the maximum fine has been imposed.”

**WHEREAS** I have read the details of the Research Project as set out in Schedule A of contract 40XXX-2X, I more specifically undertake to strictly adhere to the research objectives specified therein, and I understand that the Designated Information communicated as part of contract 40XXX-2X can be used solely to meet these objectives;

**WHEREAS** I have read Schedules D and E of contract 40XXXX-2X and shall comply with the security and confidentiality requirements therein, and I understand the implication of any breach of these requirements;

**NOW THEREFORE,** I solemnly declare that I undertake to keep secret, indefinitely, any information of which I may become aware in the course of accessing and using the information and files identified in the contract.

As a signatory, I more specifically declare that:

- I shall comply with the Institut’s confidentiality and security requirements in the course of using the information and files identified in the contract, and I undertake to read the specific instructions given by the Institut. In the event of any inconsistency or conflict between any requirements, I shall notify the Institut or my organization if notice cannot be given to the Institut, and I shall apply the most stringent instructions;
- I shall access the information and files identified in the contract only if my duties require it and circumstances justify it and solely for the purposes of the research project;
- I shall neither disclose nor make known any confidential information that I have learned and I undertake to keep this information confidential in perpetuity;
- I am fully aware that the Institut may use mechanisms to oversee information security and protection, and that any confidentiality incident on my part may lead to disciplinary sanctions;
- I am fully aware that the Institut has the right to review the use of the information and files identified in the contract for the authorized project for verification, control, protection, and information security purposes.

And I have signed: \_\_\_\_\_

NAME OF AUTHORIZED PERSON

<b>Swearing-in</b>		
Signed before me, _____ (No. _____ )		
in _____ <i>(place)</i>	this _____ <i>(date)</i>	day of _____ <i>(month and year)</i>
<i>(Signature of commissioner for oaths or legal practitioner)</i>		

## SCHEDULE D

### SECURITY AND CONFIDENTIALITY REQUIREMENTS

The security and confidentiality requirements detailed below are the minimum requirements that users of the service must adhere to for remote access to the Remote Access Microdata File (RAMF) and Intermediate Results. Work sessions will be recorded and consulted as needed by the Institut. Should users fail to comply with these obligations, the Institut reserves the right to disable remote access to the RAMF and Intermediate Results without prior notice.

**1. Concerning access to the room from which remote access takes place:**

- a) Access to the room must be controlled and limited to Authorized Persons;
- b) Access privileges must be removed as soon as an individual's duties no longer require such access.
- c) The room from which access occurs must be located in Québec. For access from a room outside the province of Québec, the Researcher and the persons authorized in Schedule B must obtain written authorization from the Institut.

**2. Each workstation allowing remote access must:**

- a) Have a current browser and a working HTTPS secure port;
- b) Not allow remote control;
- c) Use logical access controls (strong passwords) for both the computer and the network;
- d) Have functional, up-to-date antivirus software;
- e) Have approved, up-to-date security patches;
- f) Be protected by systems that can prevent physical and logical intrusions;
- g) Be locked in the absence of the Authorized Person;
- h) Be disconnected (physically and wirelessly) from any removable device with memory storage capacity (USB keys, memory cards, portable disks, optical disks, tablets, smart phones, etc.);

- i) Be available at all times for the Institut to check compliance with the terms and requirements of this contract.

3. **Each Authorized Person shall:**

- a) Make proper use of the personal identifier and security token provided by the Institut; the token will be reset annually by the Institut;
- b) Notwithstanding subsections (j) and (k), solely use mobile devices, including a cell phone, for the virtual login token application to initiate multi-factor authentication;
- c) Set a password containing 12 characters minimum, including at least three among the following: number, upper-case letter, lower-case letter, special character. This password shall be changed at least every year or as directed by the Institut;
- d) Make good use of the resources provided and not attempt to extract or load data or programs from or into the remote access environment provided by the Institut;
- e) Take the necessary measures to erase the traces of authentication codes (identifier, password, PIN, token key) from the browser's cache;
- f) Refrain from activating automatic or semi-automatic data entry or taking screenshots of the data viewed or input;
- g) Refrain from sharing or disclosing their personal identifier or token, including their password, even if temporarily or to Authorized Persons;
- h) Contact the Institut when the signing institution/organization or the Researcher requires technical support in order to obtain technical guidance and be given a debugger ID if necessary;
- i) Not allow any visitors to the Researcher's work area while remote access services are being used;
- j) Not use any application or device capable of reproducing the signals or images of the data viewed from the workstation, including but not limited to: teamwork, screen sharing, remote control, and videoconferencing applications such as Microsoft Teams, Zoom, Google Meet, Skype, and FaceTime;
- k) Use videoconferencing or screen sharing only upon prior authorization by the Institut, if the Researcher:
  - 1. only uses the assets (e.g., applications) provided by the Institut and if users make no changes to settings (e.g., functions allowed, configuration, hours of use permitted, etc.);

2. solely presents Intermediate Results, and only in the presence of persons who are already allowed access to this information. The sharing of content from a microdata file is strictly prohibited;
  3. verifies each participant, both visually and verbally, without any virtual background filter, thus allowing the duly authorized meeting facilitator to clearly identify the participants and their environment and to verify compliance with confidentiality rules, particularly the physical security of the access sites;
  4. receives the required instructions and training on access to and secure use of assets before making use of the privilege granted.
- l) Not use other peripherals (printers, projectors, etc.) capable of reproducing an image or any confidential information, regardless of the medium or process;
  - m) Ensure that results to be output from the remote access environment meet the Institut's confidentiality rules and that no result can be linked, even indirectly, to a specific individual, company, organization or association, and in this regard comply with the Institut's confidentiality procedures provided;
  - n) Immediately report to the Institut representative any anomaly or incident related to the protection of information or any change in the environment's behaviour;
  - o) Report any physical, technological or administrative event that may impact the performance of the contract or the assets of the Institut.
4. **The Institut reserves the right to:**
    - a) Check if the Researcher's activities comply with policies, guidelines and other security rules, upon reasonable notice. The check will be performed by the Institut or by any person authorized by it.
    - b) Following the compliance check, take any action it deems appropriate.
5. **Security clearance**
    - a) Any person acting under this contract must not have been convicted of a criminal or penal offence inconsistent with their functions. To this end, if deemed appropriate and as requested by the Institut, the person identified in Schedule B shall provide a security clearance or criminal background check issued by a police force and provide all necessary information to the Institut so that it can verify that this requirement is met.
    - b) Any person to be cleared or checked in this way must be jointly identified by the signing institution or organization and by the Institut at such time as the Institut deems appropriate.

**SCHEDULE E**  
**SECURITY AND CONFIDENTIALITY REQUIREMENTS**  
**IN A TELEWORK CONTEXT**

The security and confidentiality requirements detailed below are in addition to those set forth in Schedule D and are the minimum requirements that the user must comply with in a telework context. If there is any inconsistency between this schedule and other requirements, the Researcher shall notify the Institut, or otherwise shall apply the most stringent instructions. The Institut reserves the right to remove telework privileges at any time and without notice.

**1. Concerning access to the room from which telework access takes place**

- a) The premises from which telework access occurs must be located in Québec. For telework access from a room outside the province of Québec, the Researcher and Authorized Persons under Schedule B must obtain a written authorization from the Institut.
- b) Contact information for the room from which access is made as well as the telephone number of the Researcher and Authorized Persons on the research team must be provided to the Institut before access is granted. This information must be updated every time there is a change.
- c) The room must be located in the Researcher's primary or secondary residence or, in the case of Authorized Persons on the research team, at their respective home, or at a place designated by the organization as a telework location.
- d) No telework access shall be made while travelling, from public places such as restaurants, Internet cafés or common rooms, from hotel or motel rooms, from a car, on public transportation, etc.
- e) The room must meet all confidentiality and secrecy rules and requirements inherent to the nature of the sensitive information being accessed.
- f) The room and the equipment must be protected from intrusion and theft.
- g) The screen must be protected from prying eyes inside or outside.
- h) The room must be reasonably soundproof, and headphones are mandatory during calls.
- i) All access equipment including the token generator must be physically secured (locked room, locked file cabinet, locked device, etc.).
- j) The equipment must be adequately protected or locked when the room requires such protection (e.g., a room within a multipurpose hall, a living room).
- k) The equipment or room must never be left unattended while logged into a work session. Always log out or lock the session for even a small temporary break (e.g., while receiving a phone call).

- l) No equipment or application capable of capturing sounds (e.g., smart virtual assistants such as Google Home, Alexa, SIRI, Cortana, Bixby) or images (e.g., video surveillance or video conference recording system) is allowed. It is the teleworker's responsibility to choose an appropriate remote workspace and to shut down all interoperative equipment, applications and devices in order to prevent any risk of information leakage.

**2. Each workstation allowing remote telework access must:**

- a) Meet the minimum security requirements, i.e., still have technical support from the manufacturer (generally less than 10 years old) and with a recent operating system (Windows 8 or higher, MacOS 10.13 or higher);
- b) Be known in advance to the Institut (type of equipment [laptop or desktop computer, etc.]), brand, model, age and usual general specifications (operating system, etc.) as personal equipment belonging to the Researcher or to an Authorized Person on the research team; any changes must be reported to the Institut;
- c) Automatically install all security updates and all patches for hardware, operating system, antivirus and firewall (e.g., Windows firewall);
- d) Be connected to the Internet via a single home network fully controlled by the Researcher or by an Authorized Person on the research team, not a shared network (e.g., with a neighbour, someone at another address, etc.);
- e) Use, when possible, a wired Internet connection, which is deemed the safest and most stable, over a local Wi-Fi connection;
- f) Be connected to a Wi-Fi network protected by a password that is difficult to guess. The administrator account (ADMIN) to manage the router must not be the default account;
- g) Have a SSID (wireless network name) that does not contain any identifying information such as the address;
- h) Never use a public, free, or non-password-protected Wi-Fi network;
- i) Use a non-shareable, password-protected account;
- j) Immediately report to the Institut any unusual or suspicious activity or behaviour likely to cause a breach in confidentiality, or any security incident.

**3. The Institut reserves the right to:**

- a) Deny telework access to equipment if such equipment is incompatible with the services offered, if it has valid reasons to believe that security requirements may be compromised, or for any other reasonable motive at its discretion;
- b) Collect statistics on software usage and IP addresses that can enable the geolocation of where telework sessions take place;

- c) Diagnose suspicious communications, take steps to protect the network, and establish recommendations or obligations for the Researcher or any Authorized Person on the research team;
- d) Disconnect remote access without notice if it detects abnormal activity that could compromise security;
- e) Check compliance with security requirements at declared addresses or any telework access location by conducting an on-site visit with advance notice.

*Courtesy translation*