SECURE RESEARCH ENVIRONMENT SECURITY

– Policy –

1. PURPOSE

1.1 This Policy describes the security protocol regarding entry into the Secure Research Environment of the New Brunswick Institute for Research, Data and Training (NB-IRDT), and the administrative, physical, and technical safeguards in place with respect to data security.

2. SCOPE

2.1 This Policy applies to NB-IRDT Employees, Approved Data Users, Visitors, University of New Brunswick (UNB) Fredericton and Saint John campuses and Université de Moncton Security Personnel, Service Personnel, and all other persons with respect to accessing the Secure Research Environment.

3. DEFINITIONS

3.1 *Access Logbook:* A book kept at the entrance to each Secure Research Environment that serves as a permanent record of the arrival and departure of all Visitors to NB-IRDT.

3.2 *Approved Data User(s):* Individuals, such as NB-IRDT Employees, researchers, students, and government employees, who have been issued an electronic identification access card, personal identification number, and project access account following the approval of access according to all relevant NB-IRDT procedures, including a Criminal Record Check (CRC).

3.3 *Employee(s) (of NB-IRDT):* All full-time and part-time, continuing and term Employees currently earning wages or salaries from NB-IRDT (including the Director). Does not include independent contractors.

3.4 *Hub Location*: The NB-IRDT Fredericton location securely housing Personal Information in its custody as a Research Data Centre under PHIPAA and is responsible for the administration of NB-IRDT.

3.5 *New Brunswick Institute for Research, Data and Training (NB-IRDT):* A Research Data Centre as defined in RTIPPA and PHIPAA. Like other Research Data Centres, NB-IRDT has the authority to compile and link Personal Information and Personal Health Information for the purposes of research, analysis, or evidence-based decision-making. NB-IRDT has three locations, with the hub located in Fredericton, and Satellite Sites located in Saint John and Moncton. These facilities are situated on the University of New Brunswick (Fredericton) campus (Keirstead Hall, 38 Dineen Drive; Units 316, 317, and 317-A); on the Saint John campus (Hazen Hall, 93-97 Tucker

Park Road; Unit 339); and, on the Université de Moncton campus (Bibliothèque Champlain, 415 avenue de l'Université; salle 031).

3.6 *Pseudonymous Data:* Information from which direct identifiers (e.g., name, Medicare numbers, social insurance number) have been eliminated or transformed, but indirect identifiers (e.g., date a service was accessed, medical diagnosis, length of hospital stay, occupation, level of education) remain intact.

3.7 *Satellite Site(s)*: Physical facilities located in Saint John and Moncton for the Secure Research Environment where NB-IRDT Approved Data User(s) may access project-specific, De-identified, Personal Information provided through a dedicated and secure fiber optic network connection to servers at the Hub Location (Fredericton).

3.8 *Secure Research Environment (SRE)*: The infrastructure housing NB-IRDT data resources and equipment for accessing resources. The facilities are located on the University of New Brunswick (Fredericton) campus (Keirstead Hall, 38 Dineen Drive; Units 316, 317, and 317-A); on the Saint John campus (Hazen Hall, 93-97 Tucker Park Road; Unit 339); and, on the Université de Moncton campus (Bibliothèque Champlain, 415 avenue de l'Université; salle 031). The buildings housing these facilities are under respective campus security surveillance.

3.9 *Security Personnel:* Members of an NB-IRDT affiliated campus security team. Security Personnel have the authority to access the physical facilities when called for emergency or when there is suspicion of unauthorized activity.

3.10 *Service Personnel*: Custodial, maintenance, or other servicing personnel who are either Employees of an NB-IRDT affiliated University or contracted through the University, and require occasional access to carry out custodial, service provision, or maintenance duties.

3.11 *Visitor(s)*: All persons requesting or requiring access to a NB-IRDT Secure Research Environment who are *not* NB-IRDT Employees or NB-IRDT Approved Data User(s).

4. POLICY STATEMENTS

4.1 NB-IRDT is composed of three sites with NB-IRDT Fredericton, a secure Research Data Centre, serving as the Hub Location securely housing Personal Information in its custody, and two Satellite Sites serving as remote secure lab facilities where NB-IRDT Approved Data Users may access project specific De-identified Personal Information provided through a dedicated and secure fiber network.

4.1.1 The Fredericton Hub Location, located at Keirstead Hall (units 316, 317, and 317-A), 38 Dineen Drive, Fredericton, New Brunswick, consists of three main areas: the laboratory (lab) area with a series of workstations for researchers; Data Analysts workspace with computers; and the Database Administrator's office containing computers and servers that are confined in a steel cage. A locked fireproof safe, which contains data media devices, is also housed in the Database Administrator's office.

4.1.2 The Saint John Satellite Site, located at Hazen Hall (unit 339), 93-97 Tucker Park Road, Saint John, New Brunswick, and shared with a Statistics Canada Research Data Centre (CRDC), consists of two (2) main areas: a general reception and consultation area; and, a lab area for data access.

4.1.3 The Moncton Satellite Site, located in Bibliothèque Champlain, 415 avenue de l'Université, Moncton, New Brunswick, and shared with a Statistics Canada Research Data Centre (CRDC), consists of one (1) room, which serves as a Secure Research Environment data access area with staff workspace.

4.2 These three (3) physical locations in Fredericton, Saint John, and Moncton, are collectively understood to be the "NB-IRDT" or "NB-IRDT Secure Research Environment."

4.3 Multiple levels of security and safeguards, described in the following table, protect access to the workstations, staff computers, servers, and safe containing the data media devices.

4.3.1 Physical Safeguards Protecting Access to Secure Research Environment – NB-IRDT Fredericton

Security Feature	Type of Access	Who has Access*
Main Door		
Security Alarm	Code	NB-IRDT Database Administrator NB-IRDT Director NB-IRDT Systems Administrator NB-IRDT Data Analysts
Door Deadbolt	Key ("Do not copy" key)	NB-IRDT Database Administrator NB-IRDT Director NB-IRDT Systems Administrator NB-IRDT Data Analysts
Door Keypad Entry System	Code (personal identification number)	NB-IRDT Database Administrator NB-IRDT Director NB-IRDT Systems Administrator

		NB-IRDT Data Analysts NB-IRDT Employees (working hours) NB-IRDT Approved Data Users (working hours)
Electronic Identification Access Card Swipe Pad	Card	NB-IRDT Database Administrator NB-IRDT Director NB-IRDT Systems Administrator NB-IRDT Data Analysts NB-IRDT Employees (working hours) NB-IRDT Approved Data Users (working hours)
Systems Administrator's Office		
Door Lock	Key	NB-IRDT Database Administrator NB-IRDT Director NB-IRDT Systems Administrator NB-IRDT Data Analysts
Database Administrator's Office		
Door Lock	Key	NB-IRDT Database Administrator NB-IRDT Systems Administrator
Safe	Combination	NB-IRDT Privacy Officer NB-IRDT Systems Administrator
Safe	Key	NB-IRDT Database Administrator NB-IRDT Assigned Data Analyst backup
Server Cage	Key	NB-IRDT Database Administrator NB-IRDT Systems Administrator

*Fredericton Campus Security has approval to access the facility in the event of an emergency.

4.3.2 Physical Safeguards Protecting Access to Secure Research Environment – NB-IRDT Saint John

Security Feature	Type of Access	Who has Access**
Main Door		
Security Alarm	Code	NB-IRDT Data Analysts
Door Deadbolt	Key ("Do not copy" key)	NB-IRDT Data Analysts
Door Keypad Entry System	Code (personal identification number)	NB-IRDT Data Analysts (days of operation) NB-IRDT Employees (working hours) Approved Data Users (working hours)
Electronic	Card	NB-IRDT Data Analysts (days of operation)

Identification Access Card Swipe Pad		NB-IRDT Employees (working hours) Approved Data Users (working hours)
NB-IRDT Staff Office		
Door Lock	Key	NB-IRDT Data Analysts

** UNBSJ Campus Security has approval to access the facility in the event of an emergency.

4.3.3 Physical Safeguards Protecting Access to Secure Research Environment – NB-IRDT Moncton

Security Feature	Type of Access	Who has Access***
Main Door		
Security Alarm	Code	NB-IRDT Data Analysts
Door Deadbolt	Key ("Do not copy" key)	NB-IRDT Data Analysts
Door Keypad Entry System	Code (personal identification number)	NB-IRDT Data Analysts (days of operation) Approved Data Users (working hours)
Electronic Identification Access Card Swipe Pad	Card	NB-IRDT Data Analysts (days of operation) Approved Data Users (working hours)

*** Université de Moncton Campus Security has approval to access the facility in the event of an emergency.

4.4 All Campus Security Personnel have the authority to access the respective physical locations anytime throughout the day or night when called for emergency or when there is suspicion of unauthorized activity.

4.5 At the end of the day, the Database Administrator or NB-IRDT Employee ensure that: all workstations are shut down, all internal doors are locked, the safe and the server are locked (Fredericton), the site main door deadbolt is locked, and the alarm is engaged.

4.6 Access to a Secure Research Environment requires all NB-IRDT Employees and Approved Data Users to attend in house NB-IRDT Data Privacy Training once per year in keeping with the *NB-IRDT Data Confidentiality and Security Policy*.

4.7 As an operational requirement all NB-IRDT Employees and Approved Data Users (per NB-IRDT User Access Accounts Policy) must provide a Criminal Record Check (CRC) completed within a twelve (12) month prior to commencing employment or being granted Approved Data User access. CRC results are reviewed by the NB-IRDT Privacy Officer. It is however, at

the discretion of the NB-IRDT Director whether CRC findings of concern are relevant to the granting of employment or Approved Data User access.

5. PROCEDURES

5.1 Access by NB-IRDT Employees and Approved Data Users – NB-IRDT Fredericton

5.1.1 On notification of a new NB-IRDT Employee hire or Approved Data User, the NB-IRDT Systems Administrator will enter access parameters for their electronic identification access card (UNB UCard) including access start and end (contract end) dates.

5.1.2 NB-IRDT Employees are issued an electronic identification access card (UNB UCard) on employment and Approved Data Users, on project approval, are assigned campus guest status permitting them access to a guest identification access card (UNB UCard).

5.1.3 Individuals are responsible to maintain their own card and activate their personal identification number for their secure electronic identification access card (UNB UCard) using the UNB secure login portal.

5.1.4 Individuals who have lost or suspect that their electronic identification access cards have been stolen, are to notify the NB-IRDT Systems Administrator on discovery so the card can be disabled.

5.1.5 Individuals are responsible for requesting replacement cards through the Fredericton Information Technology Services (ITS) UCard office (Room 106, Marshall d'Avray Hall).

5.1.6 Upon termination of NB-IRDT employment the NB-IRDT Systems Administrator will deactivate the Employee's access card.

5.1.7 At the end of an Approved Data User's access date, the scheduled automated deactivation will remove access. If access needs to be removed prior to the preset deactivation date, the NB-IRDT Systems Administrator will deactivate the access card.

5.2 Access by NB-IRDT Employees and Approved Data Users – NB-IRDT Satellite Sites

5.2.1 On notification of a new NB-IRDT Employee hire or Approved Data User, a designated NB-IRDT Satellite Site Data Analyst will complete a new NB-IRDT Employee or Approved Data User *Security Access Request Form* and submit to the appropriate campus security contact.

5.2.2 Appropriate campus security offices will issue the secure electronic identification access card and personal identification numbers to NB-IRDT Employees and Approved Data Users.

5.2.3 Only the designated NB-IRDT Satellite Site Data Analyst, or delegate, has permission to make this request.

5.3 Secure Research Environment Use by NB-IRDT Employees and Approved Data Users – All NB-IRDT Secure Research Environments

5.3.1 NB-IRDT Employees and Approved Data Users are permitted access to only one physical location at a time based on their employment role and/or project approval.

5.3.2 NB-IRDT Employees and Approved Data Users must use their electronic identification access card and secure personal identification number for each and every entry into a physical location and must not share or loan their access card to anyone else.

5.3.3 NB-IRDT Employees and Approved Data Users can only access a Secure Research Environment when the alarm is disabled, and the deadbolt opened.

5.3.4 Approved Data Users are limited to accessing the Secure Research Environment during regular business hours when an NB-IRDT Employee is physically present; parameters for this access are administered through card privileges.

5.3.5 In the event of an NB-IRDT Employee's absence or Approved Data User's project suspension for an undetermined length of time, access to the Secure Research Environment will be deactivated and reinstated upon their return.

5.3.6 Access to the NB-IRDT Data Analysts' office (Fredericton and Saint John) and NB-IRDT Database Administrator's office (Fredericton) is permitted only when explicit permission is given and an NB-IRDT Employee accompanies the individual.

5.4 Access by Visitors

5.4.1 All Visitors must apply for access to a Secure Research Environment by completing the *Visitor Access Form*. The *Visitor Access Form* is to be completed prior to entry and must be submitted in person to NB-IRDT staff on the day of the scheduled visit. The Visitor Access Form must clearly indicate:

- The purpose of the visit;

- The NB-IRDT Employee (visit host) who will be supervising the Visitor(s); and,
- The requested date and time of the visit.

5.4.2 The visit host will review the requirements and restrictions contained in this Policy and the *NB-IRDT Mobile Device Policy* with the Visitor prior to accessing a Secure Research Environment.

5.4.3 On the day of the visit, Visitor will present, in addition to a completed *Visitor Access Form*, one piece of valid government or University of New Brunswick issued photo identification to a designated NB-IRDT Employee.

- Visitors to the NB-IRDT Fredericton Hub Location will first go to the NB-IRDT Administration Assistant (or delegate) and present one piece of photo identification. The NB-IRDT Administrative Assistant (or delegate) will contact the visit host who will escort the Visitor to the Secure Research Environment.
- Visitors to the NB-IRDT Saint John and NB-IRDT Moncton Satellite Sites will prearrange a set arrival time with the NB-IRDT Employee. On arrival, the Visitor will present photo identification to the NB-IRDT Employee with the completed *Visitor Access Form*.

5.4.4 The Visitor will sign the *Access Logbook* and indicate the date and time of the entry.

5.4.5 The Visitor will restrict their visit to the purpose described in the *Visitor Access Form* and remain in the company of the visit host at all times.

5.4.6 On exiting a Secure Research Environment, the Visitor will indicate the time of exit in the *Access Logbook*.

5.4.7 NB-IRDT Employees are not permitted to bring guests or Visitors with them when accessing the Secure Research Environment unless they have followed the processes as outlined in this policy.

5.4.8 Only NB-IRDT Employees are authorized to answer the door.

5.5 Access by Service Personnel

5.5.1 Service Personnel (UNB Facilities Management, IT Staff, etc.) will arrange a time with a NB-IRDT Employee (or delegate) prior to arriving on site.

5.5.2 Entrance on the day of service for expected Service Personnel is granted by reporting to the NB-IRDT Administration desk at the NB-IRDT Hub Location (Fredericton) or by calling the phone number posted at the entrance to the Satellite Sites.

5.5.3 All Service Personnel will complete a *Visitor Access Form* and sign the *Access Logbook* indicating the date and time of the entry, the purpose of visit, and time of exit.

5.5.4 On presentation of the appropriate photo identification, the NB-IRDT Employee will permit entry into the secure area.

5.5.5 The NB-IRDT Employee must remain with Service Personnel at all times.

5.5.6 The entrance door of the facility may not be propped open for any reason.

5.5.7 An NB-IRDT Employee will inform Personnel of the *NB-IRDT Mobile Device Policy*.

5.5.8 Service Personnel will restrict their visit to the original purpose indicated.

5.5.9 There must be no data access or approved project work occurring during service provision.

5.6 Access by Custodial Staff

5.6.1 Custodial Personnel with appropriate identification may access the facility by knocking on the door and being granted access by an NB-IRDT Employee.

5.6.2 All custodial staff will sign the *Access Logbook* and indicate the date and time of entry, purpose of the visit, and time of exit.

5.6.3 The NB-IRDT Employee must remain with custodial staff at all times.

5.6.4 The entrance door of the facility may not be propped open for any reason.

5.6.5 The NB-IRDT Employee will inform custodial staff of the *NB-IRDT Mobile Device Policy*.

5.6.6 A *Visitor Access Form* is not required for custodial staff.

5.6.7 Custodial activities will only occur during regular business hours.

5.7 Access by Shred-it

5.7.1 A calendar of scheduled Shred-it pick-up dates and a list of Shred-it driver/pick-up employees will be provided annually to NB-IRDT administrative staff and satellite Employees. Unscheduled changes in pick-up dates or changes to Shred-it employee list must be verified with the vendor prior to granting access to the SRE.

5.7.2 Only a NB-IRDT Employee may grant Shred-it employees' access to the space where the shredding console is within the physical location.

5.7.3 Entrance is granted at the Hub Location (Fredericton) by presentation of photo identification to an NB-IRDT Employee.

5.7.4 Entrance is granted at the Satellite Sites (Saint John and Moncton) by calling the phone number posted at the entrance and presentation of photo identification.

5.7.5 Shred-it employees are to send the receipt for secure destruction immediately by email at time of pick-up. Receipts are submitted to the NB-IRDT Administrative Assistant for retention.

5.7.6 All Shred-it employees will sign the *Access Logbook* and indicate the date and time of entry, purpose of visit, and time of exit.

5.7.7 The NB-IRDT Employee must remain with the Shred-it employee at all times.

5.7.8 The entrance door of the facility may not be propped open for any reason.

5.7.9 The NB-IRDT Employee will inform Shred-it employees of the *NB-IRDT Mobile Device Policy*.

5.7.10 A *Visitor Access Form* is not required for Shred-it employees.

5.7.11 Secure Shred-it service will only occur during regular business hours.

5.8 NB-IRDT Employee Absence and Short-Term Closure

5.8.1 *NB-IRDT Hub Location (Fredericton)* - A NB-IRDT Employee must be present in the physical location during all regular hours open to Approved Data Users. The NB-IRDT Database Administrator's office must remain locked during their absence. The inner NB-IRDT Data Analyst office will also remain locked if the NB-IRDT Database Administrator, Systems Administrator, or a Data Analyst, are not present.

5.8.2 *NB-IRDT Satellite Sites (Saint John and Moncton)* - Absence of all NB-IRDT Employees for 30 minutes or more requires closure of the physical location to Approved Data Users.

6. ADMINISTRATION

6.1 Accountability

6.1.1 *NB-IRDT Hub Location (Fredericton)* - The NB-IRDT Office Manager is responsible to ensure that only the approved NB-IRDT Employees obtain office keys. The NB-IRDT Systems Administrator is responsible to

ensure that only NB-IRDT Employees and Approved Data Users obtain electronic identification access cards and personal identification number access to the Secure Research Environment. The NB-IRDT Privacy Officer serves as delegate for these responsibilities.

6.1.2 *NB-IRDT Satellite Sites (Saint John and Moncton)* - The distribution of necessary facility keys to NB-IRDT Employees is administered by the respective campus Facilities Management and/or Campus Security office on request from the NB-IRDT designated staff member. Only this individual may request electronic identification access cards and personal identification number access to the Secure Research Environment for new NB-IRDT Employees and Approved Data Users.

6.1.3 NB-IRDT Employees and Approved Data Users are accountable for the proper use and protection of any keys, electronic identification access cards, and personal identification numbers used at NB-IRDT.

6.1.4 NB-IRDT Employees and Approved Data Users are responsible to:

- immediately report the loss or theft of keys to the NB-IRDT Operations Manager; and,
- immediately report the loss or theft of electronic identification access cards to the NB-IRDT Systems Administrator (Fredericton), or to respective campus security for the Satellite Sites (Saint John and Moncton).

6.1.5 Visitor hosts are responsible to ensure that:

- all Visitors have been approved to visit;
- relevant policies have been explained;
- appropriate photo identification has been provided and verified;
- Access Logbook entries are completed;
- Mobile devices are not used; and,
- Visitors are not left unaccompanied during any portion of the visit.

6.1.6 When custodial, Shred-it, or Service Personnel are present NB-IRDT Employees are responsible to ensure that:

- Relevant policies have been explained;
- Appropriate photo identification has been provided and verified;
- *Access Logbook* entries are completed;

- Mobile devices are not used; and,
- Visitors are not left unaccompanied during the length of the service provision.

6.1.7 Visitors, custodial, Shred-it, and other Service Personnel, and Security Personnel are responsible for compliance with this Policy.

6.2 Monitoring, Auditing, and Reporting

6.2.1 All NB-IRDT Employees are responsible to report any non-compliance with this Policy or security breaches (actual or attempted) to the NB-IRDT Director and Privacy Officer.

6.2.2 The NB-IRDT Director and Privacy Officer are responsible to report any security breaches at the NB-IRDT Hub Location (Fredericton) to the UNB Security & Traffic office.

6.2.3 The NB-IRDT Database Administrator at the NB-IRDT Hub Location (Fredericton) and the NB-IRDT Employees at the Satellite Sites (Saint John and Moncton) regularly monitor the activities of Approved Data Users while in the respective Secure Facilities.

6.2.4 The UNB Door Management for the Hub Location (Fredericton) and the university security offices for the respective Satellite Sites (Saint John and Moncton) will run monthly automated reports on door electronic identification access card use. Access to these reports will be provided to the NB-IRDT Privacy Officer for reporting.

6.2.5 The NB-IRDT Systems Administrator will generate monthly data access user reports for all Secure Facilities and provide access to the NB-IRDT Data Access Coordinator for reporting purposes.

6.2.6 The *Access Logbooks* kept at the Secure Facilities are retained in accordance with the appropriate record retention schedules.

6.2.7 All *Visitor Access Forms* are retained by NB-IRDT in accordance with the appropriate record retention schedules. *Visitor Access Forms* are scanned and emailed to office of the UNB Vice President (Research) monthly.

6.2.8 The NB-IRDT Privacy Officer may conduct random Audits in all NB-IRDT facilities to compare the *Visitor Access Forms* and the door electronic identification access card use with the *Access Logbook* to ensure policy compliance.

7. RELATED DOCUMENTS

- *NB-IRDT Access Logbook*

- *NB-IRDT Glossary of Data Privacy and Security Terms*
- *NB-IRDT Mobile Device Policy*
- *NB-IRDT Visitor Access Form*

8. REFERENCES

- *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05
- *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6

9. DOCUMENT VERSION, REVIEW, AND APPROVAL HISTORY

Version	**Author**	**Nature of Change**		**Date**
1.0	NB-IRDT Staff	Document Creation		September 2016
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2016	November 2016	September 2017

Version	**Author**	**Nature of Change**		**Date**
1.1	D. Curtis Maillet	Minor Revisions		June 2017
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		June 2017	June 2017	September 2018

Version	**Author**	**Nature of Change**		**Date**
2.0	D. Curtis Maillet	Major revisions for 2018 expansion		January 2019
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2019	November 2019	July 2020

2.1	NB-IRDT Staff	Updated to current formatting; changes to procedures and roles		February 2022
2.2	NB-IRDT Staff	Content edits		June 2022
2.3	NB-IRDT Staff	Content edits		May 26, 2023
Approved by VP Research UNB		**Approval Date**	**Effective Date**	**Review Date**
David MaGee		July 2023	July 2023	July 2024