USER ACCESS ACCOUNTS

– Policy –

1. PURPOSE

1.1 This Policy describes the different levels of permitted access to the Data held in New Brunswick Institute for Research, Data and Training's (NB-IRDT) custody and the processes for setting up appropriate Approved Data Users access accounts for NB-IRDT Employees and Approved Data Users.

2. SCOPE

2.1 This Policy applies to all NB-IRDT Employees and Approved Data Users.

3. DEFINITIONS

3.1 *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).

3.2 *Confidentiality Agreement (CA):* A contract signed by NB-IRDT Employees and Approved Data User(s) that describes obligations and responsibilities regarding the maintenance, Use, access to, and Disclosure of Confidential Information.

3.3 *Criminal Record Check:* A name-based record search of the local police force's Records Management System (RMS), the Provincial Justice Information System (JIS), and the Canadian Police Information Centre (CPIC) repository of criminal convictions.

3.4 *Custodian:* As defined in the PHIPAA, an individual or organization that collects, maintains, or uses personal health information for the purpose of providing or assisting in the provision of health care, and treatment, the planning, and management of the health care system, or delivering a government program or service.

3.5 *Data Business Owner:* The entity holding legal rights and control over a Data Set(s) and its variables. In the context of a Data Sharing Agreement, this is the entity (e.g., Custodian, Public Body) who has signed the Data Sharing Agreement and who has shared/disclosed a Master Data Set(s) with/to NB-IRDT.

3.6 *Data Curation:* The range of data quality assurance activities and processes necessary to ensure the integrity and utility of Data Sets (e.g., validation, data dictionary development).

3.7 *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.

3.8 *Master Data Set (Master Data)*: The original Data Set received by NB-IRDT from a Data Business Owner/Custodian, provided on an encrypted media transfer device.

3.9 *Principal Investigator*: The individual who holds principal responsibility for a research project such as a project grant recipient or the head of a laboratory, most often the lead researcher on the Data Access Request.

3.10 *Project Data*: Data prepared for a specific project and stored in a project folder, which consists only of information approved for a specific research project.

4. POLICY STATEMENTS

4.1 NB-IRDT is obligated under PHIPAA, the *Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6* (RTIPPA), and through Data Sharing Agreements with Data Business Owners/Custodians to ensure that Data is protected against unauthorized access.

4.2 Access permissions are assigned at the minimum level that will meet the needs to the task at hand and are banded to the role and/or project (e.g., if an NB-IRDT Employee performs multiple roles that require access to Data, they will have a separate Approved Data User account for each role, with appropriate permissions).

4.3 The NB-IRDT Database Administrator has the highest level of System access; they require access to Master Data Sets for the purposes of Data verification and Project Data preparation. The NB-IRDT Database Administrator creates, monitors, and deletes User accounts and permissions for all NB-IRDT Employees and Approved Data Users.

4.4 The NB-IRDT Systems Administrator has the highest level of Systems access with no project folder access. They have limited access to Master Data Sets for the receipt of new data in the absence of the NB-IRDT Database Administrator. They maintain and support NB-IRDT by facilitating and scheduling the running of reports for Monitoring User account activity, maintaining the infrastructure for secure data access, ensuring storage backup and destruction, and providing the generation of system's activity Auditing reports.

4.5 NB-IRDT Senior Data Analysts have limited highest level System access; they require limited access to the Master Data Sets so they can serve, when designated by the NB-IRDT Director and or Database Administrator, as backup to the NB-IRDT Database Administrator for the purposes of Data verification and Project Data Preparation.

Additionally, NB-IRDT Senior Data Analysts have access permission that allows access to complete data analysis and other procedures relating to the accuracy, documentation, and Curation of the Data Sets

4.6 NB-IRDT Data Analysts have access permission that allows access to complete data analysis and other procedures relating to the accuracy, documentation, and Curation of the Data Sets. NB-IRDT Data Analysts cannot access Master Data Sets.

4.7 NB-IRDT Approved Data Users only have access permissions to their own Project Data.

4.8 The NB-IRDT Privacy Officer and Data Access Coordinator have access to User account generated reports to conduct and review Audits on data Use access, but do not have access to any project folders or Data Sets.

4.9 The NB-IRDT Director has no access permissions beyond User accounts set up for approved projects that have gone through the *NB-IRDT Data Access Request* process.

4.9 Additional NB-IRDT Employees (e.g., NB-IRDT Data Transfer Coordinator, Office Manager, Research & Evaluation Manager, etc.) who do not require access to the data held in secure custody for their roles are not permitted to access the data or have a User account.

4.10 All NB-IRDT Approved Data Users and Employee access permissions are reviewed annually in tandem with annual Data Privacy Training required by the *NB-IRDT Data Confidentiality and Security Policy*.

4.11 The following table summarizes NB-IRDT roles, access permissions, and file access.

NB-IRDT Access Permissions		
NB-IRDT Role	**Permission**	**Files**
Database Administrator	• Read, write, and execute privileges to all data files. • Create Approved Data User accounts with associated privileges.	• System-wide
Systems Administrator	• Read, write, and execute privileges to all data files for IT infrastructure support. • Generate and run Data Access Audit reports. • Create Approved Data User accounts with associated privileges in Database Administrator's absence.	• System-wide
Senior Data Analyst	• Read, write, and execute privilege to all data files when appointed in Database Administrator's absence. • Read and execute privileges to approved Project Data files and Data Curation approved by the Director and Database Administrator.	• Limited System-wide • Project data folders • Curation task specific Data Sets
Data Analyst	• Read and execute privileges to approved Project Data files and Data Curation approved by the Director and Database Administrator.	• Project data folders • Curation task specific Data Sets
Research Assistant	• Read and execute privileges to approved Project Data files.	• Project Data folders
Approved Data User	• Read and execute privileges to approved Project Data files.	• Project Data folders

5. PROCEDURES

5.1 NB-IRDT Data Access

The NB-IRDT Database Administrator is responsible for providing initial Passwords to NB-IRDT Employees and Approved Data Users, as well as reporting any Password violations to the NB-IRDT Director and Privacy Officer.

5.1.1 NB-IRDT Employees as Approved Data Users

- NB-IRDT Employees working on approved data access projects are assigned a data access account when they complete Administrative Safeguards and are approved for a data project. The NB-IRDT Data Access Coordinator will email the NB-IRDT Database Administrator requesting the account be set up indicating the Employee's role and the approved project.

- The NB-IRDT Database Administrator will create a unique Approved Data User access account and assign a temporary Password.
- At first sign-in, the NB-IRDT Employee creates their own strong Password as indicated in the *NB-IRDT Passwords Policy*.
- Access to each data project requires a separate and distinct Password. Two or more projects may not be opened at the same time by the same Approved Data User on one workstation.

5.1.2 NB-IRDT Employees Performing Data Curation

- NB-IRDT Employees assigned to work on Data Curation for a Data Set or in relation to a specific project must submit a *Data Quality Access Request* form to the NB-IRDT Director (carbon copies (cc) to the NB-IRDT Database Administrator, and Privacy Officer). The request form must clearly state the Data Sets requested for Curation and the rationale for access.
- If the NB-IRDT Director feels access is warranted for curation work the request will be approved and notification will be sent to nb-irdtdata@unb.ca Footprints and assigned to the Database Administrator.
- The NB-IRDT Director will grant access for a limited time in relation to the work with a maximum access time of three (3) months from date of approval.
- If additional time is required for completion of the Data Curation work at the end of the approved access time, a *Data Quality Access Request* form must be completed requesting an extension and submitted to the NB-IRDT Director (cc to the NB-IRDT Database Administrator, and Privacy Officer).
- The NB-IRDT Database Administrator will set up a Data Curation folder with a temporary Password and will notify the NB-IRDT Employee.
- At first sign-in, the NB-IRDT Employee will create their own strong Password as indicated in the *NB-IRDT Passwords Policy*.
- Access to the folder is removed on completion of the Data Curation work.
- Data Curation work will often result in an improved or updated Data Sets accessible to NB-IRDT Employees and Approved Data Users for research work. This is a distinct Data Set from the original Master Data Set.

- Data Curation work does not include any access to, or editing of, original Master Data Sets. Any recommended edits or concerns are reviewed by the NB-IRDT Database Administrator and forwarded to the Data Business Owner/Custodian.
- Creation and development of supporting Data Set documentation (e.g., data codebook) are reviewed by the NB-IRDT Database Administrator prior to being made available to NB-IRDT Employees and Approved Data Users.

5.1.3 NB-IRDT Approved Data Users

- All individuals seeking data access for projects must go through the *NB-IRDT Data Access Request* process.
- Prior to receiving a User access account, NB-IRDT Approved Data Users must complete all Administrative Safeguards as stated in the *NB-IRDT Data Access Approval Policy*.
- When the Project Start Date has been determined, the NB-IRDT Data Access Coordinator will email the NB-IRDT Database Administrator and request that a User access account be set up for all members of the research project or Information Management team who have been approved for access to the data.
- The NB-IRDT Database Administrator will create a unique Approved Data User access account and assign a temporary Password for each member of the team. Each Approved Data User is instructed that their account is not to be shared, even with members of their own team.
- At first sign-in, an NB-IRDT Approved Data User creates a strong Password as indicated in the *NB-IRDT Passwords Policy*.

5.2 Expiration or Termination of Permissions/Accounts

5.2.1 User accounts for NB-IRDT Approved Data Users are assigned for the length of the approved project with a maximum of three (3) years (the standard project duration). Principal Investigators are required to apply for project extensions if necessary.

5.2.2 User accounts for NB-IRDT Approved Data Users are reviewed annually to ensure project activity requires ongoing access. To maintain Approved Data User accounts, all NB-IRDT Employees and Approved Data Users must complete annual data privacy training in keeping with the *NB-IRDT Data Confidentiality and Security Policy*.

5.2.3 On notification from the NB-IRDT Research and Evaluation Manager, the NB-IRDT Data Access Coordinator (cc the NB-IRDT Finance

Coordinator) of the completion of a research project, the NB-IRDT Director will inform the NB-IRDT Database Administrator to terminate the Approved Data Users' access permissions related to that project.

5.2.4 Annual update reports are required by the University of New Brunswick (UNB) Research Ethics Board for ongoing projects. Principal Investigators are responsible for their own annual reporting to the Research Ethics Board.

5.2.5 On notification from the NB-IRDT Director of an Employee's long-term absence (cc to the NB-IRDT Data Access Coordinator), the NB-IRDT Database Administrator will deactivate the Employee's account, which is to be reinstated on their return once the NB-IRDT Employee's Data privacy training and security and orientation training have been updated.

5.2.6 On notification from the NB-IRDT Director of an Employee's termination of employment (cc to the Data Access Coordinator), the NB-IRDT Database Administrator will deactivate the Employee's account.

5.2.7 In the event of a Privacy Incident or Breach, the NB-IRDT Database Administrator will suspend related account(s) in accordance with *NB-IRDT Privacy Breach Policy*.

5.2.8 Deletion of Approved Data User accounts and project folders is in keeping with the *NB-IRDT Record Retention and Destruction Schedule*.

5.2.9 NB-IRDT does not create "group" or "multi-person" Approved Data User access accounts. Shared project folders can be accessed by all persons approved for a particular project; however, individuals must sign in using their own unique account and Password.

5.2.10 User accounts are not to be shared or used by anyone other than the individual who has been assigned the account.

6. ADMINISTRATION

6.1 **Accountability**

6.1.1 The NB-IRDT Director is responsible for the identification and approval of access permissions (or changes thereto) of NB-IRDT Employees and Approved Data Users.

6.1.2 The NB-IRDT Database Administrator is responsible to grant, modify, deactivate, or terminate Approved Data User access

permissions/Approved Data User accounts, and to evaluate and monitor compliance with access permissions granted.

6.1.3 The NB-IRDT Systems Administrator is responsible to manage the IT infrastructure and to grant, modify, deactivate, or terminate Approved Data User access permissions/Approved Data User accounts for the NB-IRDT Database Administrator, as well as generate data Use reports for Auditing of Approved Data Users and NB-IRDT Database Administrator access permission compliance.

6.1.4 The NB-IRDT Data Access Coordinator is responsible to ensure that the Principal Investigator of approved projects has signed a Data Access Agreement with UNB Office of Research Services as required in the policies and procedures of NB-IRDT.

6.1.5 The NB-IRDT Data Services Coordinator is responsible to ensure that NB-IRDT Employees and Approved Data Users have completed all Administrative Safeguards as required in the policies and procedures of NB-IRDT.

6.1.6 All NB-IRDT Employees and Approved Data Users are individually accountable to follow data privacy and security safeguards while accessing and using NB-IRDT information and information technology resources.

6.1.7 All NB-IRDT Employees and Approved Data Users are required to comply with the Confidentiality and protection of privacy provisions of this policy.

6.1.8 Should projects end sooner than anticipated, Principal Investigators are responsible to inform the NB-IRDT Data Access Coordinator of the completion of the project to ensure that Approved Data User Access Permissions are terminated in a timely manner.

6.2 **Monitoring, Auditing, and Reporting**

6.2.1 The NB-IRDT Database Administrator keeps a log of all NB-IRDT Employees and Approved Data Users, as well as their Approved Data User accounts.

6.2.2 NB-IRDT Database Administrator and Systems Administrator generate monthly Data access Audits to monitor Approved Data User access to assigned project folders.

6.2.3 Reports are made available to the NB-IRDT Data Access Coordinator for review and preparation of monthly access and data usage reports forwarded to the NB-IRDT Privacy Officer.

6.2.4 The NB-IRDT Privacy Officer prepares monthly Secure Research Environment access Audit reports to monitor User access. Audit reports

are informed by security reports provided by UNB Fredericton IT for the secure facility in Fredericton and similar reports are generated by the respective security departments of the host universities for the Saint John and Moncton Satellite Sites.

6.2.5 The NB-IRDT Privacy Officer compiles a yearly review and annual report on User data access as required under the originating and operating agreements with the Department of Health. These are delivered at the end of each fiscal year.

6.2.6 A random system of Auditing may be conducted for identification of any unauthorized access or attempts at unauthorized access to data. Random Audits are conducted on access to approved projects and by random selection of NB-IRDT Employees and Approved Data Users. Any unauthorized access identified is immediately reported to the NB-IRDT Director and the appropriate *NB-IRDT Privacy Breach Policy* procedures are followed.

6.2.7 NB-IRDT Employees are instructed to report any instances of improper Use or sharing of Approved Data User access accounts to the NB-IRDT Privacy Officer.

7. RELATED DOCUMENTS

- *NB-IRDT Data Access Approval Policy*
- *NB-IRDT Data Access Request Form*
- *NB-IRDT Data Confidentiality and Security Policy*
- *NB-IRDT Data Quality Access Request Form*
- *NB-IRDT Glossary of Data Privacy and Security Terms*
- *NB-IRDT Passwords Policy*
- *NB-IRDT Privacy Breach Policy*

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
2.0	D. Curtis Maillet	Minor Revisions for 2018 Expansion		January 2019
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2019	November 2019	July 2020

Version	Author	Nature of Change		Date
3.0	NB-IRDT Staff	Update to current formatting; changes in procedures and accountability roles		February 2022
3.1	NB-IRDT Staff	Content review – slight grammatical & spacing change		June 30, 2022
3.1.1	NB-IRDT Staff	Content review and addition of roles and backup responsibilities		May 26, 2023
Approved by VP Research UNB		**Approval Date**	**Effective Date**	**Review Date**
David MaGee		July 2023	July 2023	July 2024