1. PURPOSE

1.1 The purpose of this policy is to guide NB-IRDT employees and approved users on how to proceed in the event of a privacy breach, and to demonstrate to stakeholders that a systematic procedure is in place to respond to and deal with a privacy breach.

1.2 A privacy breach occurs when: (i) there is an unauthorized access, use, disclosure, copying, modification, retention, disposal or destruction of personal information or personal health information; (ii) personal information or personal health information is stolen or lost; or (iii) there is unauthorized entry to the NB-IRDT Secure Facility.

1.3 Activity is considered to be unauthorized if it occurs in contravention of applicable privacy legislation (Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6 (RTIPPA) and Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05(PHIPAA), NB-IRDT policies and procedures and/or contractual agreements with New Brunswick government or data owners.

1.4 Privacy breaches also include publishing data and analysis that could lead to the identification (either alone or with other information) of subject individuals, publishing cells smaller than 5, or removing data outside the secure NB-IRDT system contrary to data sharing agreements.

2. SCOPE

2.1 This policy applies to all data-related inquiries, all NB-IRDT employees and approved users, all members serving on NB-IRDT committees, senior University Administration, and Government of New Brunswick employees serving in advisory capacities to NB-IRDT (e.g. UNB Vice President Research, NB-IRDT Advisory Board, Executive Committee, etc.).

3. DEFINITIONS

3.1 Data Owner: The originating Department, public body or other organization from which the data were provided.

3.2 Privacy Audit: A systematic review and evaluation of privacy practices to measure ongoing compliance with privacy best practices and applicable provincial and federal privacy legislation. It includes following privacy practices through the data life cycle (identification, compilation, access, disclosure and final disposition of data) to identify gaps or potential gaps in data handling practices that may lead to a privacy breach.

3.3 Privacy Incident Report: A report resulting from the completion of the NB-IRDT Record of Breach – Information on Discovery Form.

3.4 Use: To handle or deal with the information; this includes reproducing the information but does not include disclosing the information.
4. POLICY STATEMENTS

4.1 NB-IRDT is committed to protecting the privacy, confidentiality and security of the personal information and personal health information in its databases, and has policies and procedures designed to prevent a privacy breach. All NB-IRDT employees and approved users will receive privacy and confidentiality training, which include the process for handling a suspected or confirmed breach.

4.2 Upon the discovery of a personal health information breach, the NB-IRDT Privacy Officer (“Privacy Officer”) will, at the first reasonable opportunity, notify the New Brunswick Access to Information and Privacy Commissioner (“Commissioner”) as required by PHIPAA.

4.3 The protocol described below provides a systematic approach for managing a breach including notification, containment, documentation, investigation, additional notification and follow up remedial action.

5. PROCEDURES

The general order of events that occurs upon discovery of a privacy breach or suspected breach is identified in Flowchart 1. However, it is acknowledged that logistics may require some tasks be completed simultaneously or in a different order.

Flowchart-1

- Discovery
- Containment
- Investigation
- Notification of Affected Individuals
- Follow up Action

5.1 The following five steps are followed upon discovery of a privacy breach or a suspected privacy breach:

Step 1: On Discovery of the Breach

5.1.1 The person who discovers the breach will immediately notify the Database Administrator, NB-IRDT Director, and Privacy Officer, or designates.

5.1.2 The discoverer will document the following information:

- Project title and number (if relevant)
- Date and time of discovery
- Who was involved (if known)
• Estimated date and time privacy incident/breach occurred (if possible to estimate)
• Type of privacy incident/breach (e.g., unsecured password, loss, theft, inadvertent disclosure, maintenance of data past destruction, etc.) The discoverer describes the situation but does not make the determination whether the situation constitutes an incident or a breach.
• Type of data involved (e.g., included direct personal identifiers, encrypted data)

5.1.3 The Privacy Officer will notify the University Secretary and the Records Management, Access and Privacy Coordinator (“UNB Privacy Coordinator”), NB-IRDT Systems Administrator, and the applicable data owner(s).

5.1.4 In the event of a personal health information breach the Privacy Officer will notify the Commissioner and provide the following information:
• Her/his contact information;
• A description of the nature of the breach;
• The date and location of the breach; and
• The date the breach came to the attention of the Privacy Officer.

**Step 2: Containment**

5.1.5 The process of containment is to be initiated as soon as possible to prevent release or further release of personal information or personal health information. Steps toward containment are taken by the first person who becomes aware of the breach and has the ability and authority to do so. Some of these steps can be taken by the discoverer and/or Privacy Officer whereas others require intervention by the NB-IRDT Database Administrator, the Director and/or the Systems Administrator.

5.1.6 The containment processes includes:
• Determine what, if any, information has been disclosed.
• Retrieve as much of the breached information as possible (ideally all breached information).
• Ensure no copies of personal information or personal health information have been made or retained by the unauthorized person.
• Ensure that additional breaches cannot occur through the same means.
• Determine whether the privacy breach would allow unauthorized access to any other personal information or personal health information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system) to contain the situation.
Privacy Breach Policy

- Document all above information and be prepared to review with the Privacy Officer.

5.1.7 The following steps are intended to illustrate the actions that may be required to contain the breach or suspected breach – but are not exhaustive. Individual circumstances can dictate the particular requirements.

- If an electronic data device is stolen from NB-IRDT, notify security and the police immediately to determine if the person who removed the device is still in the building.
- Confirmation of email addresses and fax numbers will be made before sending any personal information.
- If a fax was sent to the wrong number, call the recipient and ask them to destroy the document and to confirm in writing that the document was securely destroyed, that no copies were made or kept, and that information will not be shared in any circumstances.
- If an email was sent to the wrong person, call the recipient and ask them to securely destroy any email printouts that were made and delete the email and to confirm in writing that the document was securely destroyed, that no copies were made or kept, and that information will not be shared in any circumstances.
- If an unauthorized person has or may have access to a database or computer system, notify the Database Administrator, who can disable accounts or change passwords and identification numbers.
- Where unauthorized verbal disclosure has occurred, request that the recipient of the personal or sensitive information treat it confidentially.

Step 3: Investigation and Documentation

5.1.8 The NB-IRDT Director, Privacy Officer and Database Administrator will investigate the breach, and initiate procedures and impose sanctions consistent with relevant UNB policy.

5.1.9 Breach investigations include the following elements:

- Interviewing individuals involved with the privacy breach or individuals who can provide information about the process and confirm details on the Record of Privacy Breach Form;
- Ensuring any issues surrounding containment and notification have been addressed by NB-IRDT; and
- Obtaining any relevant evidence.

5.1.10 The Privacy Officer (or designate) is responsible for the documentation of the breach and will complete the Record of Privacy Breach Form.
Step 4: Notification of Affected Individuals

5.1.11 The Privacy Officer in conjunction with the Commissioner (when appropriate), the UNB Privacy Coordinator and appropriate data owner(s), will determine whether notification to individuals to whom the information relates is possible and/or required. Any notification may be completed jointly with the data owner and/or the UNB Privacy Coordinator.

5.1.12 Exemption to notification regarding personal health information may occur only if none of the following three situations as stated in section 49(2) of PHIPAA will occur as a result of the breach. Notification is not required if the breach will not:

- have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates.
- have an adverse impact on the mental, physical, economic or social well-being of the individual to whom the information relates.
- lead to the identification of the individual to whom the information relates.

Step 5: Follow up Action

5.1.13 In accordance with section 63 of PHIPAA, the Commissioner may investigate notices of privacy breach involving NB-IRDT. In such an event, the Privacy Officer will cooperate fully with the Commissioner to:

- Review the steps taken to contain the breach;
- Ensure the notification of affected individuals (as applicable);
- Review the circumstances surrounding the breach in an attempt to fully understand the scope and cause of the breach;
- Determine appropriate corrective mitigating measures to reduce future risk; and
- Follow and implement recommendations for corrective measures as provided by the Commissioner.

5.1.14 Upon completion of the Investigation, a plan will be developed to identify the root cause(s) of the breach and implement corrective and preventative measures (prevention plan). The following list of preventive measures is intended to illustrate the actions that may be taken, but it is not an exhaustive list. Individual circumstances will dictate the required actions.

- Determine whether the privacy breach protocol was followed.
- Conduct a security audit of administrative, physical and technical safeguards and correct any deficiencies.
- Educate NB-IRDT employees and approved users on how to avoid similar breaches.
Privacy Breach Policy

• If the privacy breach was due to a discrepancy between policy and practice, educate all relevant persons to ensure greater awareness of the expected practices (based on the existing policies).
• If the privacy breach was due to a weakness in an existing policy, revise the policy and notify all relevant persons about the revision.
• Review the privacy and security training program to identify and rectify gaps.

5.1.15 Where an NB-IRDT employee caused the breach, the applicable UNB Employee Agreement will be consulted regarding discipline and appropriate sanctions made.

5.1.16 In the situation where a non-employee of NB-IRDT was the cause of the privacy incident/breach, the NB-IRDT Director will inform the individual’s employer or faculty advisor (if a student) of the circumstances of the breach in writing in a timely manner.

5.1.17 NB-IRDT reserves the right to disallow access to NB-IRDT data for persons who have been the cause of a privacy breach.

6. ACCOUNTABILITY

6.1 All NB-IRDT employees and approved users are responsible to immediately report a suspected or confirmed breach of privacy / security to the appropriate person and follow the protocol as the discoverer of the breach.

6.2 The NB-IRDT employee, Director, Privacy Officer and/or Database Administrator is responsible to ensure proper containment of the breach; provide appropriate notification; document and report; take action to prevent future breaches and follow up with monitoring and audits as listed in Section 7 below.

6.3 The Privacy Officer is responsible to report the breach to the data owner(s) and the Commissioner under PHIPAA, ensure all appropriate documentation is completed and signed, assist with the investigation as required, notify others as required and conduct the review and develop and /or implement the remedial plan.

6.4 The NB-IRDT Director is responsible to notify the relevant employer /faculty advisor and to follow the appropriate UNB processes and provincial legislation penalties.

7. MONITORING, AUDITING AND REPORTING

7.1 Following any privacy breach investigation, the NB-IRDT Director and Privacy Officer will review this policy to determine its effectiveness and revise accordingly.

7.2 The Privacy Officer and/or Database Administrator will conduct an audit following a privacy / security breach to ensure that any planned changes to procedures / processes have been implemented.
7.3 On a bi-annual basis, the Privacy Officer will submit reports to the NB-IRDT Director and the Executive Director of the UNB Office of Research Services of any privacy and/or security breaches or issues, describe how the situations were addressed and indicate proposed actions for preventing future issues.

7.4 In accordance with the Originating Agreement and the Operating Agreement with the Government of New Brunswick, and any master data sharing agreements with data owners, on an annual basis the NB-IRDT Director will provide each data owner the following:

1. A report providing a list of all persons who were approved to access NB-IRDT data along with the purpose for the access.
2. A summary of the risks identified through current Privacy Impact Assessment and Threat and Risk Assessment.
3. A summary of any changes to its operating procedures, governance structure, privacy or security policies or protocols.

Copies of items 2 and 3 will also be provided to the Office of the Access to Information and Privacy Commissioner on an annual basis.

8. **QUESTIONS**

8.1 Questions or concerns regarding this policy or privacy obligations at NB-IRDT can be directed to the Privacy Officer at NB-IRDTprivacy@unb.ca.