National Cybersecurity Consortium

Data Management Procedure

Ultimate Recipients

www.ncc-cnc.ca

Related Policy

Data Management Policy – Ultimate Recipients
Intellectual Property Policy

Purpose

The National Cybersecurity Consortium (NCC) Data Management Procedures - Ultimate Recipients documents minimum requirements Ultimate Recipients must follow to demonstrate compliance with the NCC Data Management Policy – Ultimate Recipients and supports the NCC's data management activities related to its funding program.

Objective

The objective of this Procedure is to outline for Ultimate Recipients (URs) their responsibilities with regards to data management. It includes a data management plan template that can be used by the URs and references best practices from various industry sectors that can be used to guide the development of a UR's data management plan for any projects submitted to the NCC for funding.

Approval and authority

The NCC's Board approves this Procedure and any revisions or amendments to this Procedure. The Procedure is reviewed on a bi-annual basis in consort with any effected Policies.

Authority for operationalization of this Procedure resides with the NCC's Executive Director (ED).

Definitions

Designated groups: refers to the following designated groups under the federal *Employment Equity Act*: women, people with disabilities, Indigenous peoples, and visible minorities.

Eligible project intellectual property: means all intellectual property (IP) conceived, produced, developed, or reduced to practice in carrying out eligible funded projects considered for funding by the NCC, or by an ultimate recipient (UR) and/or any affiliated person(s) of the UR, or any of their employees, agents, contractors or assigns.

Funding program: the NCC's funding program has three streams of focus - research and development, training, and commercialization.

Project: refers to a project that receives funding from the NCC's funding program.

Security breach: means any act or omission that materially compromises the confidentiality, integrity, and availability of data.

Service provider: means a third party with whom a UR, or one of the participants involved in a project, has entered into agreements for services, facilities and/or infrastructure that are necessary to support project activities.

Ultimate Recipient (UR): project lead who receives funding from the NCC.

UR Funding Agreement (URFA): means the agreement entered between the NCC and a UR.

Data management requirements

The following section outlines the NCC's requirements of URs in relation to data management.

Data management plans

Using the attached *Data Management Plan Template for Ultimate Recipients,* the NCC requires URs to develop a data management plan that addresses the following:

Collection*:* establishes guidelines on what data are collected, how it is treated and used, the format of collected data, and on how the data are structured to ensure standardization;

Collaboration: articulates how data are managed in a project in which URs collaborate with one or more entities;

Governance*:* ensures authorities and associated accountabilities are implemented through policies, procedures, guidelines and succession plans (as required);

Integrity, Reliability, and Availability*:* establishes a common structured data format and data exchange technologies, standards, and guidelines for the storage, backup, and retention of data, as well as for validating its authenticity, and the processes for ensuring its timely, efficient, and accurate retrieval;

Ownership: establishes a clear ownership structure for the collection, production, and sharing of data (and where consent must be provided);

Privacy*:* identifies privacy laws and ensures that the URs, and any associated project participants, have legal authority to collect, use, or disclose personal information; that they always safeguard personal information; and that the rights and obligations provided for in the application of privacy laws are given effect;

Sharing*:* articulates how agreements are implemented to ensure interoperability of and accessibility to the data by authorized parties; and

Traceability*:* ensures traceable access to data within Canada.

Data collection, access and usage
Except as otherwise permitted or required by applicable law or regulation, URs only: (i) collect and use data that constitute personal information for the purpose the data was provided; and (ii) retain data that constitute personal information for as long as necessary to fulfill the purposes for which URs collected the data, including for the purposes of satisfying any legal, accounting, or reporting requirements.

URs, and the participants involved in their project, must use best practice approaches to anonymize data to ensure personally identifying information is removed when it is not needed for a clearly defined purpose. The protection of privacy rests solely on the UR to ensure that anonymity is maintained to the greatest extent possible and in conformance with any relevant privacy and data protection legislation and/or regulations.

At the NCC's sole discretion, the NCC may request that, prior to the disclosure and/or transmission of any data related to an identifiable person by URs to the NCC, the URs provide the NCC with any information that the NCC may need to enable it to evaluate and determine whether it is authorized to accept and/or receive such data. Any determination by the NCC that it is unable to accept such data does not constitute non-compliance under the NCC's Data Management Policy – Ultimate Recipients or a breach under the UR Financing Agreement.

Designated groups
The NCC recommends that URs develop a self-identification process for members of designated groups that is culturally respectful and that ensures that participants feel safe in disclosing their identity(ies) and that their information is protected and used appropriately.

URs who work with data created in the context of research by and with First Nations, Métis, and Inuit communities, collectives, and organizations, must ensure the data are managed according to principles developed and approved by those communities, collectives, and organizations, and in partnership with them.

Evaluation
The NCC is committed to reviewing UR data management plans to ensure they meet the requirements outlined in this Procedure.

As the NCC is committed to continuous improvement and learning in relation to data management plans, the NCC will review the data management plans developed as part of its first round of projects, identify lessons-learned, and will use this information to make improvements to its data management template. Over time, it will also develop an approach to the evaluation of data management plans.

Intellectual property
All IP derived from data, including anonymized data, datasets, labelled data, representations, trained models and outputs, are considered eligible project IP and subject to the commitments and requirements of the NCC's Intellectual Property Policy.

Location and protection
URs must confirm that both their data as well as those of any participants involved in their project are hosted on servers located in Canada. URs must also confirm that they are maintaining appropriate technical and organizational security measures to protect data from unauthorized loss, use, disclosure, alteration, or access and are complying with any security measures that may be specified by their institution/organization and the NCC.

If URs and/or any participants involved in their project retain the services of a third-party service provider for the hosting of their data, the data must still be hosted on servers and facilities in Canada that are owned, controlled, and operated by the third-party provider. URs and any participants involved in their project must use reasonable efforts to ensure that the service provider is subject to information security controls at least substantially similar to those required under the UR Financing Agreement.

Monitoring
URs are responsible for ensuring that project data are tracked and monitored on an ongoing basis and in a manner that is consistent with their data management plans.

Point of contact
The NCC requires URs to identify an individual who is the project's point-of-contact regarding all project-related activities and issues, including data management.

Reporting
The NCC requires URs to submit progress reports to their NCC program officer as part of their quarterly financial reporting. Specifically, URs are asked to indicate in their quarterly reports whether the project has encountered any data issues. If data issues have occurred, the UR is then asked to identify solutions for addressing those data issues and to report on progress and/or resolution in the subsequent quarterly financial report. In addition, URs are required to summarize in their project's annual progress report any data issues, how those issues were resolved, and any changes to the UR's data management plans.

The NCC program officer is responsible for notifying the Director, Grant Administration and Membership (DGAM) if any of the project's data issues or changes to the data management plan merit consideration at a higher level. The DGAM oversees actions for resolving notable data issues to ensure the project is in compliance with the NCC's data management requirements.

Security breach
URs and the participants involved in their project must notify the NCC without undue delay and within twenty-four (24) hours of becoming aware of a security breach. This notice shall minimally include a description of the:

- nature of the security breach, including the type and number of data targeted by the security breach;
- likely consequences of the security breach on the data; and

- measures taken or proposed to be taken by URs and the participants involved in their project to address the security breach, including, where appropriate, measures to mitigate possible adverse effects.

Once the NCC has received notification of a breach, the NCC will notify its funders as per the requirements outlined in any agreements the NCC may have with those funders.

To the extent that such information is not available at the time of the notice to the NCC regarding said security breach, URs and the participants involved in their project must follow-up with the NCC as information becomes available, to ensure full disclosure of the security breach without undue delay. The URs and the participants involved in their project must document responsive actions taken in connection with any security breach and must conduct a post-incident review of events and actions taken. Findings of this post-incident review must be shared by the UR with the NCC.

Types of data
The NCC requires URs to identify the various types of data within their project (e.g., confidential data, data protected by IP rights, data that can be made public) and how these different data types are accessed, managed, and safeguarded.

Amendment: The Operational Leadership Committee may amend this procedure.	Last Review:
Approval Date:	Last Revision: