National Cybersecurity Consortium Data Management Policy

Ultimate Recipients

www.ncc-cnc.ca

Related Procedures

Data Management Procedure – Ultimate Recipients

Purpose

The National Cybersecurity Consortium (NCC) Data Management Policy - Ultimate Recipients governs and supports the NCC's data management activities related to its funding program.

Objective

The objective of this Policy is to outline for ultimate recipients (URs) their responsibilities with regards to data management. It is accompanied by a data management plan template that URs are required to complete and by guidelines to support them in this work.

Approval and authority

The NCC's Board approves this Policy and any revisions or amendments to this Policy. The Policy is reviewed on a bi-annual basis.

Ultimate authority for operationalization of this Policy 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 projects funded 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 Financing Agreement (URFA): means the agreement entered into between the NCC and a UR.

Statement of commitment

The NCC encourages URs and their project teams to make their data openly available whenever possible and to adopt the "FAIR" principles through which the Findability, Accessibility, Interoperability and Reuse of data is promoted. However, the NCC also recognizes that a significant proportion of the data collected and developed by URs are sensitive in nature and that they may involve intellectual property (IP) and privacy concerns. The NCC, therefore, recommends that URs develop measures for managing access and acquiring consent.

The NCC requires URs to commit to ensuring that data management planning is undertaken at all stages of a project that involves data - from inception through to design and completion - and that data management plans are an essential part of this work.

URs must clearly articulate and document their data management plans and processes and provide the following:

- documentation for any ethics oversight required to acquire, store, or use data throughout its lifecycle;
- methods for collecting and sharing data (format, structure);
- roles, responsibilities, and processes for data decision-making and ownership;
- methods for ensuring data integrity, reliability, and availability; and
- processes for ensuring the traceability of data.

URs must also ensure an appropriate level of protection for data assets including safeguards for the privacy of personal information.

Cybersecurity

The NCC requires URs to ensure that their data management measures are aligned with their institutional/organizational cybersecurity policies and processes, as well as any cybersecurity requirements that may be specified by the NCC.

In addition, URs must abide by applicable laws and other binding authorities such as standards, accreditations, and professional orders, as well as NCC policies and procedures. In addition, they must respect the Tri-Agency's Statement of Principles on Digital Data Management, its Research Data Management Policy, and all other related documentation.

Warrantees

URs and the participants involved in their project must represent and warrant that they have all necessary third-party consents, permissions, and rights required by any applicable laws or policies to provide access, storage, use, reproduction, and sharing of its data.

Non-compliance

The NCC's Director of Grant Administration and Membership (DGAM) has authority over the process for investigating non-compliance with this Policy.

The NCC may suspend or revoke funding if URs are found to be non-compliant with this Policy.

Amendment: The Board may amend this policy.	Last Review:
Approval Date:	Last Revision: