

Responsible AI Framework



Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
Board of Directors	107-00-00	ICES Network	ICES Network	N/A
Original Date (YYYY-MM-DD)	Current Version (YYYY-MM-DD)	Review Frequency	Next Review (Month YYYY)	Supersedes (if applicable)
2026-07-23	2026-07-23	Annual	July 2027	N/A
Authority (Title)		Board of Directors		
Framework Owner (Title)		Executive Team		
Required Reviewers (Titles)		[None]		

Please refer to the [glossary](#) for bolded terms and their definitions.

Provisions highlighted in grey are not yet in effect.

1.0 PURPOSE

- 1.1 As a trusted data steward with a robust and mature data governance framework, ICES is poised to facilitate responsible innovation and the implementation of trustworthy and responsible **Artificial Intelligence (“AI”)**, including but not limited to **Machine Learning (“ML”)** and **Generative AI (“GenAI”)**.
- 1.2 At the same time, real innovation requires risk-taking. ICES should enable **ICES Agents** to take risks, safely and in the context of a robust risk management framework. ICES should also accept that while not all efforts at innovation will succeed, done properly they can fail without jeopardizing trust.
- 1.3 The increasing breadth and depth of **ICES Data** as well as the research/analytics, science, and data expertise within the ICES community are important foundations for innovation within ICES.
- 1.4 Equally important and foundational are ICES core mission, vision, and values, and the organizational priority placed on the social determinants of health and health equity for the overall well-being of Canadians.
- 1.5 The aim of this *Responsible AI Framework* is to foster innovation efforts across all of ICES, including those in AI, so that they can be more effectively coordinated and implemented, and remain aligned with the values, priorities, and commitments of ICES – all the whilst, continuing to be demonstrably accountable to the public.
- 1.6 Specifically the framework establishes:
 - 1.6.1 the key goals for driving innovation at ICES;
 - 1.6.2 the governance principles to guide the development, implementation, use, and evaluation of **AI Systems** and **AI Activities** across the **ICES Network**;

Responsible AI Framework

- 1.6.3 a foundation for AI risk management such that paths to minimize potential negative impacts of AI Activities along with opportunities to maximize positive impacts are identified; and
- 1.6.4 accountability for the use of **ICES Information**, which includes **ICES Data** and **Corporate Information**, to support AI Activities.

2.0 SCOPE

- 2.1 This framework situates and provides a foundation for **Responsible AI Governance** at ICES, which includes policies, standards, procedures, tools, and guidelines. As per ICES' *Policy Governance Framework*, such documents apply to all ICES Agents.¹

3.0 ACCOUNTABILITY AND GOVERNANCE

- 3.1 ICES' Board of Directors are accountable for ICES' *Responsible AI Framework*.
 - 3.1.1 The Board of Directors address risks that may negatively affect ICES' ability to protect the privacy and security of individuals whose **Identifiable Information** is received and to maintain the confidentiality of that information. This includes AI Activities.
- 3.2 ICES' Executive Team is responsible for ensuring that ICES has a Responsible AI Governance that is demonstrably accountable to the public.
- 3.3 ICES' Executive Team may delegate certain responsibilities to its senior management teams to ensure that all AI Activities are tracked, logged, and implemented in accordance with this framework and associated policies, standards, and procedures.

4.0 DETAILS

4.1 ICES' AI Position Statement

- 4.1.1 ICES' AI Position Statement, as set out in Appendix "A", is a high-level statement that guides ICES on the purpose for adopting AI and inform ICES Agents, the public, interest holders, rights holders, and partners about ICES' approach to AI implementation.
- 4.1.2 The Board should review the AI Position Statement on an annual basis.
- 4.1.3 Amendments to the AI Position Statement may be approved by the Board at any time and is not restricted to only during an annual review cycle.

4.2 Key goals driving AI Activities

Goal for AI Activities	Description
1. Accelerate science and discovery	<i>Increasing complexity of the data ICES collects and uses requires careful decision-making and investments based on clear priorities. ICES will create greater capacity for innovative science and data through targeted investments.</i>

¹ See the *ICES Governance and Operations Charter* for a description of ICES' Policy Governance Framework.

Responsible AI Framework



2. Remain a trusted data steward when implementing novel technologies and methodologies	<i>As pressure to innovate increases, risks should be understood and managed, and safeguards and controls should be respected and effective.</i>
3. Broaden and deepen the types of data and tools available	<i>Addressing health equity and overall well-being of Canadians requires data on the social factors that affect individual health outcomes. ICES needs to broaden the types of data it collects to improve health outcomes. In addition, discovery science and health system analytics, including in AI, will increasingly require more complex clinical data, as well as new domains of data.</i>
4. Remain accountable to key interest holders, rights holders, and partners, including Indigenous organizations and communities, equity-deserving communities and the broader public	<i>ICES will remain trustworthy through meaningful dialogues with partners in respect of impactful AI Activities.</i>
5. Build and strengthen relationships with AI and related innovation partners and interest holders	<i>Working with academic and private sector organizations will be important to develop new capacity especially in areas such as AI, data management and federated analytics. In all cases the ways in which ICES engages third parties should be transparent, align with ICES mission, vision, and values, and not undermine trust.</i>
6. Attract and retain excellent staff, researchers and students	<i>At ICES, people are its greatest strength. ICES will continue to invest in supporting teams to achieve outstanding results, such that they adapt to, engage with, and drive innovation at ICES.</i>
7. Improve service delivery through modernization and automation of internal processes and upskilling, including implementing AI Systems and AI Activities.	<i>ICES should continually innovate in its internal processes and operations to increase efficiency and value for money. By innovating processes, ICES should aim to provide ever-better client services.</i>

4.3 AI principles at ICES

4.3.1 These key goals driving AI Activities should be framed within a context of Responsible AI Governance, adhering to core, basic tenets to guide policies, standards, procedures and practices.

4.3.2 The following are ICES' principles for guiding any AI Activity:

AI PRINCIPLES	
1	RELIABILITY AND SAFETY AI Activities should not endanger human life and health, and should continue to provide ICES a social license to utilize data for the benefit and improvement of health and health outcomes. This includes measuring how ICES' AI Activities may impact natural resources, the environment, and communities.
2	PRIVACY COMPLIANT AI Activities should not compromise ICES' designation under legislation and its reputation as a trusted data steward (avoiding unlawful collection, use, disclosure, retention, and destruction). The dignity of the person should be preserved when ICES Data or Corporate Information is leveraged for AI Activities.
3	SECURITY RESILIENT Any data utilized to train AI models should be protected from leaks or disclosures and AI Systems should be resistant to compromise and attacks.
4	UNDERSTANDING AND MANAGING BIASES IN DATA AI Activities should aim to understand and manage biases in data based on demographics and other factors to ensure the AI Activities will equitably benefit all persons. Efforts to manage risks should account for these biases, recognizing and acknowledging that these cannot guarantee equity and fairness.
5	TRANSPARENCY AND EMPOWERMENT When ICES Data and Corporate Information is utilized for AI Activities, appropriate information, conveyed in a manner that takes into account the digital literacy of the person, should be enabled and shared with the public.
6	CANADIAN DATA SOVEREIGNTY AND INDIGENOUS DATA SOVEREIGNTY AI Activities at ICES should align with Canadian data sovereignty to ensure any ICES Data and Corporate Information used in AI Systems remains primarily subject to Canadian law. ICES also respects the principle of Indigenous Data Sovereignty and aims to incorporate the principle in ICES' approach to data governance and AI Activities that impact Indigenous Data.

7

ACCOUNTABILITY AND RISK-BASED DECISION-MAKING

There should be clear responsibility assigned for AI Activities such that any risks identified have assigned owners who are accountable for mitigating such risks.

8

OVERSIGHT MECHANISMS

AI Activities should be monitored during and after deployment to align with the principles set out in this framework, the *Responsible AI Policy*, and other associated policies, standards, and procedures.

The above principles for this *Responsible AI Framework* reflect the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) as well as data sovereignty considerations.

4.4 Ongoing review of this framework

4.4.1 Due to the evolving and shifting trends in AI, ICES' *Responsible AI Framework* should be reviewed at least annually by ICES' Board of Directors.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Responsible AI Policy* (forthcoming)

5.2 Standards

5.3 Procedures

5.4 Tools

5.5 Guidelines

6.0 TRAINING AND COMMUNICATION

6.1 This framework is available on the **ICES Intranet**.

6.2 This framework is communicated to all **ICES Agents** across the **ICES Network** during onboarding and on a yearly basis.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 ICES Agents must comply with this framework.

7.2 All non-compliance may be subject to a range of **Disciplinary Actions** in accordance with applicable policies, including:

7.2.1 *Discipline and Corrective Action Policy*

7.2.2 *Termination of Employment Policy*

7.2.3 *Discipline and Corrective Action in Relation to ICES Data Policy*

7.2.4 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*

Responsible AI Framework



7.3 Compliance is subject to audit in accordance with applicable policies, including:

7.3.1 *Privacy and Security Audit Policy*

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this framework must be in accordance with applicable policies, including:

8.1.1 *Ongoing Review of ICES' Policy Suite Policy*

8.1.2 *Change Management and Exceptions Policy*

8.2 Exceptions cannot relieve ICES of its legal requirements, including but not limited to those established under:

8.2.1 *Personal Health Information Protection Act, 2004 ("PHIPA")* and its regulation;

8.2.2 *Coroners Act* and its applicable regulations;

8.2.3 *Child, Youth and Family Services Act, 2017 ("CYFSA")* and its applicable regulations; and

8.2.4 The **IPC Manual**, **Coroners Addendum**, and **CYFSA Addendum**.

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	Change Notes
2026-07-23	■ Framework created.

Responsible AI Framework



Appendix A

AI Position Statement (forthcoming)