Ongoing Review of ICES' Policy Suite Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	003-00-00	ICES Network	ICES Network	All Acts
Original Date (YYYY-MM-DD)	**Current Version** (YYYY-MM-DD)	**Review Frequency**	**Next Review** (Month YYYY)	**Supersedes** (if applicable)
2022-09-30	2025-10-31	Triennial	October 2028	2025-07-31

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	Director, Cybersecurity

Please refer to the **glossary** for bolded terms and their definitions.

Provisions highlighted in grey are not yet in effect and are subject to review and approval by the Information and Privacy Commissioner.

1.0 PURPOSE

1.1 This policy ensures that ICES' policies, standards, and procedures – together ICES' **Policy Suite** – are reviewed on an ongoing basis in order to determine on a regular basis when amendments may be necessary or new policies, standards, or procedures are required.

1.2 ICES' policy governance and these ongoing reviews are informed by ICES' responsibilities as a Prescribed Entity under:

1.2.1 *Personal Health Information Protection Act ("PHIPA")*

1.2.2 *Coroners Act*

1.2.3 *Child, Youth and Family Services Act ("CYFSA")*

2.0 SCOPE

2.1 This policy applies to ICES' Policy Suite as part of overarching policy governance within the organization.

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Privacy and Legal Officer ("CPLO")

3.1.1 Ensures ICES' Policy Suite is reviewed every three years in advance of ICES' triennial reviews by the Information and Privacy Commissioner of Ontario ("**IPC**").

3.2 Legal Services

3.2.1 Manages policy governance at ICES, including:

(a) Initiating and coordinating reviews of policies, standards, and procedures, in accordance with this policy;

(b) Tracking and logging information related to changes to ICES' Policy Suite; and

(c) Monitoring exceptions requested to existing policies, standards, and procedures, via the process set out in the *Change Management and Exceptions Policy*

3.3 Department Heads

3.3.1 Review policies, standards, and procedures that they are the Owners or Required Reviewers for, in order to identify changes required to existing documents or when new documents are necessary to address emerging activities at ICES.

3.4 Director, Privacy and Legal Office ("**PLO**") / Director, Cybersecurity

3.4.1 Conduct reviews of all privacy-related and security-related policies, standards, and procedures on no less than an every three year cycle.

3.5 Project Management Office ("**PMO**")

3.5.1 Oversee the change management process at ICES.

4.0 DETAILS

4.1 Frequency of review

4.1.1 At a minimum, Legal Services must ensure policies, standards, and procedures are reviewed by the month and year identified as the "Next Review" on the applicable document. This date varies based on the frequency of reviews of a particular policy, standard, or procedure.

4.1.2 At a minimum, ICES' Policy Suite that relates to ICES Data, including privacy and security policies, standards, and procedures, must be reviewed every three years.

4.1.3 Procedures should be reviewed more frequently to address any process changes that may have arisen in the organization.

4.2 Review considerations

4.2.1 When reviewing Policy Suite documents to determine if amendments or other changes are necessary, reviewers must have regard for:

(a) Any relevant orders, decisions, guidelines, fact sheets, and best practices issued by the IPC and the courts under *PHIPA*, the *Coroners Act*, and/or the *CYFSA,* or their regulations.

(b) ICES' compliance requirements as a Prescribed Entity, as set out in the **IPC Manual, Coroners Addendum**, and the **CYFSA Addendum**.

(c) Evolving industry privacy standards and best practices.

(d) Amendments to PHIPA, the *Coroners Act*, the *CYFSA*, and their regulations that may be relevant to ICES as a Prescribed Entity.

(e) Findings and recommendations arising from **Compliance Audits, Security Audits**, **Privacy Impact Assessments ("PIAs"), Privacy Breaches**, and/or **Security Incidents.**

(f) Findings and recommendations arising from triennial reviews by the IPC.

4.2.2 Reviews must also consider:

(a) Maintaining alignment amongst ICES' Policy Suite to ensure contradictory information is not being provided to ICES Agents.
(b) The operational needs of the organization to ensure processes implemented through ICES' policies, standards, and procedures are sustainable, effective, and support ICES' mission, vision, and values.

4.3 Review process

4.3.1 Legal Services (typically the Senior Legal Counsel / Regulatory Legal Advisor) must engage the Department Heads who are Owners and Required Reviewers of ICES' Policy Suite.

4.3.2 Department Heads must review their applicable documents to confirm accuracy to operational needs or if changes are necessary.

4.3.3 During this process, Legal Services must ensure no revisions cause misalignment amongst existing Policy Suite documents or impacts ICES' legal and regulatory obligations.

4.4 Policy Suite approval process

4.4.1 Revisions to ICES' Policy Suite and introduction of new policies, standards, and procedures are subject to approval in accordance with the *Change Management and Exceptions Policy*.

4.4.2 Legal Services and PMO facilitate this review and approval process.

4.5 Communication to ICES Agents

4.5.1 Legal Services coordinates with PMO to ensure approved changes to ICES' Policy Suite are communicated to ICES Agents, which, at a minimum, includes announcing in ICES' weekly communication to all ICES Agents.

4.6 Public Transparency as a Prescribed Entity

4.6.1 Regard must be had for ICES' obligations set out in the *Public Transparency as Prescribed Entity Policy*. Changes to key privacy policies also need to be communicated publicly via ICES' website.

4.7 Exceptions tracking

4.7.1 Legal Services is responsible for monitoring requested and approved exceptions to ICES' Policy Suite, which are handled in accordance with the *Change Management and Exceptions Policy*.

4.7.2 When monitoring, consideration should be given to whether:

(a) A pattern of exceptions requests suggests gaps in the existing Policy Suite that may need to be addressed; or

(b) Exceptions that may impact ICES' legal and/or regulatory obligations.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Change Management and Exceptions Policy*

5.1.2 *Public Transparency as a Prescribed Entity*

5.2 Standards

5.3 Procedures

5.4 Tools

5.5 Guidelines

6.0 TRAINING AND COMMUNICATION

6.1 Policies**,** standards**,** and procedures are available on the **ICES Intranet**.

6.2 This policy and any related standards and/or administrative procedures are communicated to all **ICES Agents** across the **ICES Network** during onboarding and on a yearly basis. Policy awareness is also supported and promoted by the policy's **Owner**.

6.3 Once new policies**,** standards**,** and procedures are published to the ICES Intranet, they are communicated to ICES Agents on the **ICES Intranet** and through ICES' weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 ICES Agents must comply with all applicable policies, standards, and procedures.

7.2 ICES Agents must notify a Privacy and/or Security **Subject Matter Expert ("SME")** at the first reasonable opportunity if they breach or believe there has been a breach of ICES' privacy and security policies**,** standards**,** or procedures in accordance with applicable policies and standards, including:

7.2.1 *Privacy Breach Management Policy*

7.2.2 *Security Incident Management Standard*

7.3 Enforcement of compliance with this policy is the responsibility of the ICES Agent identified as the Authority of this policy.

7.4 All violations of policies**,** standards**,** and procedures may be subject to a range of **Disciplinary Actions** in accordance with applicable policies, including:

7.4.1 *Discipline and Corrective Action Policy*

7.4.2 *Termination of Employment Policy*

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

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

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

7.5.1 *Privacy and Security Audit Policy*

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this policy 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**
2025-07-31	■ Updated title: ○ Previous: *Ongoing Review of Privacy and Security Policies, Standards, Procedures, Practices, and Exceptions Policy* ○ Updated: *Ongoing Review of ICES' Policy Suite Policy* ■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ IPC Manual: ▪ 01-02: Policy, Procedures, and Practices for Ongoing Review of Privacy Policies, Procedures, and Practices ▪ 02-02: Policy, Procedures, and Practices for Ongoing Review of Information Security Policies, Procedures, and Practices ○ Coroners Addendum: ▪ 05-02: Policy, Procedures and Practices for Ongoing Review of Privacy Policies, Procedures and Practices ▪ Part 2 – Additional Requirements ■ Updated to reflect: ○ Current processes, including identifying responsibilities carried out by Legal Services ○ Revised document template and standardized language in Sections 6.0 to 9.0 ■ Revised glossary terms and titles of ICES policies, standards, and procedures
2025-10-31	■ Revised to incorporate CYFSA-related information and revised to be clearer about review steps and processes.