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	2025-07-31	Triennial	July 2028	PO.002
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal Officer			
Required Reviewers (Titles)	Director, Cybersecurity			
	Senior Director, Research, Data & Financial Services			

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

1.0 PURPOSE

1.1 The purpose of this policy is to ensure that:

1.1.1 ICES' policies, standards, and procedures – together ICES' **Policy Suite** - are reviewed in accordance with:

(a) The Information and Privacy Commissioner of Ontario's ("IPC") requirements for ICES' designation as a **Prescribed Entity ("PE")** under:

(i) The *Personal Health Information Protection Act, 2004 ("PHIPA")* and its regulations; and

(ii) The *Coroners Act*and its regulations;

(b) The *Privacy and Security Audit Policy*; and

(c) The *Consolidated Log Policy*.

1.2 Ongoing reviews determine on a regular basis whether amendments are needed or whether new policies, standards, or procedures are required.

1.3 Exceptions to ICES' Policy Suite - are identified, approved, tracked, and logged in accordance with and in consideration of the following policies:

1.3.1 *The Consolidated Log Policy;*

1.3.2 *The Change Management and Exceptions Policy; and*

1.3.3 *The Risk Management Policy.*

2.0 SCOPE

2.1 This policy applies to all the policies, standards, and procedures in ICES' Policy Suite

2.2 This policy also applies to all exceptions approved to ICES' Policy Suite, as set out in the *Change Management and Exceptions Policy*.

3.0 ROLES AND RESPONSIBILITIES

3.1 The Chief Privacy and Legal Officer ("CPLO") is responsible for ensuring that ICES' Policy Suite is reviewed every three years and as required if there are revisions required in order to comply with this policy.

3.2 Legal Services is responsible for managing the policy governance at ICES, including:

3.2.1 Initiating and coordinating review of policies, standards, and procedures in accordance with this policy;
3.2.2 Tracking and logging approved Exceptions; and
3.2.3 Reviewing Exceptions on a quarterly basis to identify if changes are necessary to any of ICES' Policy Suite.

4.0 DETAILS

4.1 Review

4.1.1 At a minimum, the CPLO and the Director, PLO and/or the Director, Cybersecurity, as applicable, must ensure that privacy and security Policies, Standards, Procedures, Practices, and Exceptions are reviewed using the following criteria:

(a) Regard to any orders, guidelines, fact sheets and best practices issued by the IPC under PHIPA, the Coroner's Act, and their applicable regulations;

(b) Evolving industry privacy and security standards and best practices, including technological advancements in the security industry;

(c) Amendments to *PHIPA*, the *Coroners Act*, and their applicable regulations;

(d) Findings and recommendations arising from:

(i) Compliance Audits and Security Audits as per the *Privacy and Security Audit Policy*;
(ii) Privacy Impact Assessments ("PIAs"), and;
(iii) investigations into Privacy Complaints, Privacy Breaches, and Information Security Incidents;

(e) Findings and associated recommendations arising from triennial reviews from the IPC;

(f) Recommendations arising from ICES' designated insurance provider;

(g) Recommendations arising from Threat Risk Assessments ("TRAs");

(h) Exceptions; and

(i) Risks set out in the Risk Register.

4.1.2 If revisions or amendments are necessary, privacy and security Policies, Standards, Procedures, and Practices must continue to be consistent with ICES' actual day-to-day Practices, and ICES must resolve any ambiguities or inconsistencies between and among privacy and security Policies, Standards, Procedures, and Practices implemented.

4.1.3 Any revisions to Policies, Standards, Procedures, or Practices must be introduced as soon as reasonably practicable, having regard to the impact and likelihood of the risk materializing as set out in the Risk Management Standard.

4.2 Communication

4.2.1 The CPLO is responsible for ensuring amended or newly developed privacy and security Policies and Standards are communicated to the ICES Operations Committee via email. Such responsibility may be delegated to the Director, PLO or the Director, Cybersecurity as necessary.

4.2.2 Legal Services is responsible for ensuring amended or newly developed Policies, Standards, Procedures, or Practices are communicated to ICES departments or the broader ICES Network, including the ICES Operations Committee, via email and/or organizational-wide email newsletters and/or the ICES Intranet and/or in- person meetings.

5.0 RELATED DOCUMENTATION

5.1 Policies
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 Incident and Privacy Breach Management Policy*

7.2.2 *Security Incident Management Standard*

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

7.3.1 *Discipline and Corrective Action Policy*

7.3.2 *Termination of Employment Policy*

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

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

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

7.4.1 *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 Privacy and Security Policies, Standards, Procedures, Practices, and Exceptions Policy*

8.1.2 *Change Management Policy*

8.2 Exceptions cannot relieve ICES of its legal requirements, including but not limited to those established under **PHIPA**, the *Coroners Act*, their applicable regulations, or the **IPC Manual** and/or the **IPC Addendum**.

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	**Change Notes**