Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.002	ICES Network Policy	ICES Network	All Acts
Original Date (month yyyy)	**Last Review Date** (month yyyy)	**Frequency of review** (month yyyy)	**Next Review Due Date** **(month yyyy)**	**Supersedes** **(if applicable)**
September 2022	N/A	Triennially	September 2025	N/A

Authority (Title)	Policy Owner (Title)
Chief Privacy and Legal Officer	Director, PLO

Required Reviewers (Titles)		
Director, Cybersecurity	Sr. Director, Research, Data & Financial Services	

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

1.0 PURPOSE

1.1 The purpose of this **Policy** is to ensure that:

1.1.1 Privacy and security **Policies**, **Procedure**s, and **Practices** 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 Ontario's ***Personal Health Information Protection Act*** ("**PHIPA**"), the *Coroners Act*, and their applicable regulations;

b. ICES' *Privacy and Security Audit Policy*; and

c. ICES' *Maintaining a Consolidated Log of Recommendations Policy*,

such that the review determines whether amendments are needed or whether new privacy and/or security **Policies**, **Procedures,** and **Practices** are required.

1.1.2 Exceptions in respect of privacy and security **Policies**, **Procedures**, and **Practices** are identified, tracked, and logged in accordance with and in consideration of:

a. ICES' *Change Management Policy* and ICES' *Maintaining a Consolidated Log of Recommendations Policy*; and

b. ICES' *Risk Management Policy*, ICES' *Risk Management Standard*, and ICES' *Risk Management Procedure*.

2.0 SCOPE

2.1 This **Policy** applies to all privacy and security **Policies**, **Procedures, Practices,** and **Exceptions** implemented by ICES.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Privacy and Legal Officer** ("**CPLO**") is responsible for ensuring that privacy and security **Policies** and **Practices** are reviewed every three years and as required if there are revisions required in order to comply with this **Policy**.

3.2 ICES Director, **Privacy and Legal Office** ("**PLO**") is responsible for ensuring that **Procedures** are reviewed annually and as required if there are revisions required in order to comply with this **Policy**.

3.3 ICES Director, **Project Management Office** ("**PMO**") is responsible for ensuring that **Exceptions** with respect to privacy and security **Policies**, **Procedures**, and **Practices** are tracked and logged.

3.4 ICES Legal Counsel is responsible for reviewing **Exceptions** on a quarterly basis and advising ICES Director, **PLO** if changes are necessary to any **Procedures** and advising the ICES **CPLO** if changes are necessary to any **Policies**.

4.0 DETAILS

4.1 Review

4.1.1 At a minimum, the ICES **CPLO** and the ICES Director, **PLO** and/or the ICES Director, Cybersecurity, as applicable, must ensure that privacy and security **Policies**, **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. Recommendations arising from privacy audits and security audits as per ICES' *Privacy and Security Audit Policy*;

e. Recommendations arising from **Privacy Impact Assessments** ("**PIAs**"), consultations, and investigations into privacy complaints, **Privacy Incidents**, **Privacy Breaches**,

Security Incidents, and **Security Breaches** as per ICES' *Maintaining a Consolidated Log of Recommendations Policy*;

f. Recommendations arising from ICES' designated insurance provider;

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

h. Exceptions set out in ICES' **Privacy and Security Exception Log**; and

i. **Risks** set out in ICES' **Enterprise Risk Register** ("**ERR**") or **Department Risk Register** ("**DRR**").

4.1.2 If revisions or amendments are necessary, privacy and security **Policies**, **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**, **Procedures**, and **Practices** implemented.

4.1.3 Any revisions to **Policies**, **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 ICES' *Risk Management Standard*.

4.2 Communication

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

4.2.2 ICES Director, **PLO** or the ICES Director, Cybersecurity, as the case may be, is responsible for ensuring amended or newly developed **Policies, Procedures**, or **Practices** are communicated to ICES departments or the broader **ICES Network**, including the **ICES Operations Committee**, via email and/or newsletters and/or **ICES Intranet** and/or in-person meetings.

4.2.3 Any such communication must be reviewed by the ICES **CPLO**.

5.0 RELATED DOCUMENTATION

5.1 Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy

5.2 *Change Management Policy*

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

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

5.5 *Privacy and Security Incident Breach Management Policy*

5.6 *Risk Management Standard*

5.7 *Maintaining a Consolidated Log of Recommendations Policy*

5.8 *Risk Management Policy*

5.9 *Risk Management Procedure*

Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy

6.0 TRAINING AND COMMUNICATION

6.1 **Policies** and **Procedures** are available on the **ICES Intranet**.

6.2 This **Policy** and any 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 Owner**.

6.3 Once new **Policies** are published to the **ICES Intranet**, they are communicated to **ICES Employees** in ICES OnTap, the weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 **ICES Agents** must comply with all applicable ICES **Policies** and **Procedures**.

7.2 **ICES Agents** must notify an ICES Privacy **Subject Matter Expert ("SME")** or ICES Security **SME** at the first reasonable opportunity if they breach or believe there has been a breach of ICES' privacy and security **Policies** or **Procedures**, in accordance with ICES' *Privacy and Security Incident Breach Management Policy* and associated **Procedures**, as set out in the framework posted on the ICES **PLO**/Cybersecurity site on the **ICES Intranet**.

7.3 All other violations under ICES privacy and security **Policies** and **Procedures** may be subject to a range of **Disciplinary Actions** including warning, temporary or permanent loss of **Access Privileges**, legal sanctions and/or termination of employment for cause, or contract with ICES pursuant to *ICES' Discipline and Corrective Action in Relation to ICES Data Policy* and ICES' *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy* and associated **Procedures**.

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this **Policy** must be in accordance with ICES' *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy* and ICES' *Change Management Policy*.