Privacy and Security Training and Awareness Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.007	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)**
June 2014	September 2022	Triennially	September 2025	800PR-PR-004

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

Required Reviewers (Titles)		
Director, Cybersecurity		

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

1.0 PURPOSE

1.1 Privacy and security training and awareness is a **Key Control** for ICES' privacy accountability. In order for **ICES Agent** and **Third Party Service Provider ("TPSP")** training to be used as a component of demonstrable accountability, ICES must be able to characterize the training content as "evidence" of how ICES carries out its obligations as a **Prescribed Entity** under Ontario's *Personal Health Information Protection Act* **("PHIPA"),** Ontario's *Coroners Act*, and their regulations applicable to **Prescribed Entities**. This **Policy**:

1.1.1 Establishes the requirements and mandated content for privacy and security training and awareness at ICES.

1.1.2 mandates all **ICES Agents** and **TPSPs** receive privacy and security training.

2.0 SCOPE

2.1 This **Policy** applies to all **ICES Agents** and **TPSPs**.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Privacy and Legal Officer ("CPLO")** is responsible for overseeing the creation of privacy and security training materials and sustaining and standardizing privacy awareness at ICES.

3.2 The ICES **CPLO** is accountable for ensuring that all **ICES Agents** complete ICES privacy and security orientation upon onboarding and annually thereafter to fulfill their contractual obligations while acting as agents of ICES.

3.3 The ICES **CPLO** is accountable for ensuring that all **TPSPs** complete ICES privacy and security orientation upon onboarding to fulfill their contractual obligations as service providers to ICES.

3.4 **ICES Agents** and **TPSPs** must be aware of their responsibilities to protect privacy at ICES and to comply with privacy and security awareness requirements set out by the ICES **CPLO**. Such

obligations are set out in the **ICES Agent and Confidentiality Agreement ("ICES Agent CA")** and agreements executed between ICES and **TPSPs**.

4.0 DETAILS

4.1 Mandated content in training material

4.1.1 ICES' privacy and security training program shall include an overview of:

a. ICES' duties and responsibilities arising from its designation as a **Prescribed Entity** under s.18(1) of O. Reg. 329/04 under **PHIPA** and s.2 of O. Reg. 523/18 under the *Coroners Act*;

b. The **ICES Agent CA**, its purpose, key provisions, and the consequences of breach;

c. ICES' privacy and security programs and their management;

d. ICES' key privacy and security **Policies**, **Procedures**, activities, **Key Controls**, and administrative, technical, and physical safeguards to protect **Personal Health Information ("PHI") and Personal Information ("PI")** against theft, loss, and unauthorized use, disclosure, copying, modification or disposal, as well as individuals' roles and responsibilities in upholding them;

e. Role-based privacy and security related duties and obligations when implementing the administrative, technical, and physical safeguards, and how to apply the privacy and security **Policies**, **Procedures**, and **Practices** in **ICES Agents'** and **TPSPs'** day-to-day employment, contractual or other responsibilities;

f. The types and sources of **PHI/PI** collected by ICES;

g. The purposes for which ICES collects **PHI/PI** and associated legal authorities and obligations;

h. Limits on use of **PHI/PI**;

i. **Risks** associated with working in remote environments and associated controls and safeguards, including **Situational Awareness** and **Privacy Aware Environments**;

j. Details for handling **Privacy Inquiries** and **Privacy Complaints** and requests to disclose **PHI/PI**; and

k. ICES' *Privacy and Security Incident Breach Management Policy* and the role and responsibilities in identifying, reporting, containing, and participating in the investigation and remediation of **Privacy Incidents, Privacy Breaches, Security Incidents, and Security Breaches**.

4.1.2 ICES' privacy and security training program must include role-based training to ensure that **ICES Agents** understand how their roles sustain privacy compliance, what is relevant from a privacy protective perspective and why certain limitations, safeguards, and **Key Controls** are necessary for their duties.

4.1.3 ICES' privacy and security awareness program must be reviewed at least annually to ensure current and accurate content.

4.2 Delivery of privacy and security training

4.2.1 ICES' privacy and security training at onboarding must be delivered by an ICES Privacy **Subject Matter Expert ("SME"),** unless training is delivered via an e-learning module.

4.2.2 ICES' annual privacy and security training is delivered via an e-learning module.

4.2.3 At the discretion of the ICES **CPLO**, further privacy and security training may be delivered as needed.

4.3 Mechanisms for privacy and security awareness

4.3.1 ICES' privacy and security awareness program shall include mechanisms to sustain awareness and communicate significant changes, including:

a. New privacy and/or security **Policies**, **Procedures**, and **Practices**;

b. Recommendations and/or **Risks** identified in **Privacy Impact Assessments ("PIAs")** or **Threat Risk Assessments** ("**TRAs**");

c. Security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks, and reviews of system control and audit logs;

d. Evolving industry trendings, threats, and best practices;

e. Compliance audits and/or compliance monitoring and reviews;

f. **Privacy Inquiries** and/or **Privacy Complaints;** and

g. **Privacy Incidents**, **Privacy Breaches**, **Security Incidents**, and/or **Security Breaches**.

4.3.2 Awareness shall include annual workshops for role-based privacy, security, and data management teams across the **ICES Network** to illustrate how the **Risk Universe** would apply to different **Risk** scenarios, including the nature of the relevant **Risk** and the ways in which **Risk** may be managed in these ICES program areas.

4.3.3 Awareness may be delivered at ICES monthly network-wide meetings and other departmental meetings.

4.3.4 Awareness may be provided via ICES weekly network-wide communication channels, including newsletters, **ICES Intranet** content, security simulations, or through other departmental updates.

4.4 Tracking

4.4.1 Attendance and completion of privacy and security orientation upon onboarding must be tracked and logged in the "Privacy Awareness Attendance Log for Initial Privacy Orientation".

4.4.2 Attendance and completion of the yearly *Privacy and Security Awareness and Training* e-module must be tracked and logged in the "Training Completion Tracking Log".

4.5 Remediation

4.5.1 The ICES **CPLO** at their discretion may require an **ICES Agent** or **TPSP** to undergo additional privacy and/or security training if there are violations due to human error or operational **Policy**, **Procedure**, **Practice** gaps or deficiencies.

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 *Privacy and Security Audit Policy*

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

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

5.6 *Privacy and Security Incident Breach Management 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**.

7.4 Compliance is subject to annual audit by an ICES Privacy **SME** or ICES Risk & Compliance Analyst pursuant to the **Annual Audit Schedule** established under ICES' *Privacy and Security Audit Policy*.

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*.