Privacy and Security Training and Awareness Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	007-00-00	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)
2014-06-01	2025-10-31	Triennual	October 2028	2025-07-30
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 terms and 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 Privacy and security training and awareness is a **Key Control** for ICES' privacy accountability.

1.2 In order for **ICES Agent** 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:

1.2.1 The *Personal Health Information Protection Act ("**PHIPA**")* and its regulations;

1.2.2 The *Coroners Act* and its regulations; and

1.2.3 The *Child, Youth and Family Services Act ("**CYFSA**")* and its regulations.

1.3 This policy:

1.3.1 Establishes the requirements and mandated content for privacy and security training and awareness at ICES;

1.3.2 Establishes the requirements for tracking and logging completion of privacy and security training; and

1.3.3 Mandates all ICES Agents receive privacy and security training.

2.0 SCOPE

2.1 This policy applies to all ICES Agents.

2.2 References to **Identifiable Information** in this policy are only with regards to when the Identification Information is **ICES Data**, namely:

2.2.1 **Personal Health Information ("PHI");**

2.2.2 **Personal Information ("PI");** and

2.2.3 **Other Identifiable Data**.

2.3 References to **De-Identified Information** in this policy are only with regards to when the Identifiable Information is ICES Data, namely:

2.3.1 **Non-Identifiable Data**;

2.3.2 **Aggregate Data (Summary Output);** and

2.3.3 **Publishable Data.**

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Privacy and Legal Officer ("**CPLO**")

3.1.1 Oversees all privacy and security training activities, including but not limited to:

(a) Training materials;

(b) Delivery of the training; and

(c) Sustaining, standardizing, and implementing privacy and security awareness initiatives at ICES.

3.1.2 Ensures that all ICES Agents complete initial privacy and security training, and complete it on an annual basis thereafter, at minimum, as part of their obligations as ICES Agents.

3.2 ICES Agents

3.2.1 Ensure they understand their responsibilities to protect privacy at ICES; and

3.2.2 Comply with the privacy and security training requirements set out by the CPLO, as well as the privacy and security-related obligations set out in any applicable agreements, such as the **ICES Agent and Confidentiality Agreement ("ICES Agent CA").**

4.0 DETAILS

4.1 Delivery of privacy and security training

4.1.1 Initial Training

(a) All ICES Agents must complete their initial privacy and security training prior to being given any access to **ICES Data**, including but not limited to Identifiable Information.

(b) ICES' initial privacy and security training is delivered via an e-learning module.

4.1.2 Ongoing Training

(a) All ICES Agents must, at a minimum, complete privacy and security training on an annual basis.

(b) Ongoing training is delivered via an e-learning module.

(c) At the discretion of the CPLO, further privacy and security training may be delivered as needed.

4.2 Access to ICES Data

4.2.1 At minimum, ICES Agents are prohibited from being granted access to ICES Data, including Identifiable Information, until they have:

(a) Completed initial privacy and security training; and

(b) Executed an ICES Agent CA in accordance with the *ICES Agent Policy*.

4.3 Mandatory privacy and security training content

4.3.1 At minimum, initial and ongoing privacy training must include the information set out in Appendix A.

4.3.2 At minimum, initial and ongoing security training must include the information set out in Appendix B.

4.4 Maintenance of the privacy and security training program

4.4.1 The privacy and security training program (and related training material) must be reviewed on no less than an annual basis, as further set out in the *Privacy and Security Training and Awareness Procedure.*

4.4.2 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.

4.4.3 The content of any of ICES' privacy and security training must be formalized and standardized and be based on evolving privacy and information security industry standards and best practices.

4.5 Logging privacy and security training

4.5.1 Completed initial and annual privacy and security training must be logged and tracked. One or more logs may be used.

4.5.2 At minimum, the log(s) must include the required content set out in Appendix C.

4.5.3 The Director, Privacy and Legal Office ("**PLO**"), is responsible for ensuring the completed log(s) comply with this policy.

4.5.4 The log(s) are updated and maintained in accordance with the *Policy and Security Training and Awareness Procedure.*

4.6 Remediation

4.6.1 The CPLO at their discretion may require an ICES Agent to undergo additional privacy and/or security training if there are violations due to human error or operational policy, standard, and procedure gaps or deficiencies.

4.7 Privacy and security awareness

4.7.1 ICES' privacy and security training program must include mechanisms to:

(a) Foster a culture of privacy and security;

(b) Raise awareness of the privacy and security programs at ICES; and

(c) Raise awareness of the privacy and security policies, standards, and procedures, :

4.7.2 Privacy and security awareness initiatives may include but are not limited to:

(a) 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;

(b) Privacy and/or Security **Subject Matter Experts ("SMEs")** attending ICES monthly network-wide meetings and other departmental meetings to discuss privacy and/or security related topics; and

(c) ICES weekly network-wide communication channels, including newsletters, content on the **ICES Intranet**, security simulations, or through other departmental updates.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *ICES Agent Policy*

5.2 Standards

5.3 Procedures

5.3.1 *Privacy and Security Awareness Procedure*

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 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**
2025-07-30	■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ IPC Manual: ▪ Policy, Procedures, and Practices for Privacy Training and Awareness ▪ Log of Completion of Initial and Ongoing Privacy Training ▪ Policies, Procedures, and Practices for Information Security Training and Aawareness ▪ Log of Completion of Initial and Ongoing Information Security Training ○ Coroners Addendum: Part 2 – Additional Requirements ■ Re-organized content to move training content requirements and log requirements to Appendices. ■ Provisions added regarding ongoing review of the privacy and security training materials. ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0
2025-10-31	■ Revised to include CYFSA-related content; revised to reflect updated ICES Information classification terms.

Appendix A

Initial and Ongoing Privacy Training - Content Requirements

1. Status as a Prescribed Entity	
Initial privacy training must include the following information about ICES' status as a prescribed entity:	
	Description of ICES' prescribed entity status under *PHIPA*
	Description of ICES' prescribed entity status under the *Coroners Act*
	Description of ICES' prescribed entity status under the *CYFSA*
	Description of ICES' responsibilities arising from its prescribed entity status'
2. Nature of the Identifiable Information	
Initial privacy training must include the following information about Identifiable Information collected and used by ICES:	
	Description of the nature of the PHI collected by ICES
	Description of the nature of the PI collected by ICES under the *Coroners Act*
	Description of the nature of the PI collected by ICES under the *CYFSA*
	Description of the nature of Other Identifiable Data collected by ICES
	Description of whom ICES typically collects Identifiable Information from
	Explanation of the purposes that ICES collects and uses Identifiable Information for
	Explanation of how ICES' collection and use of PHI is permitted under *PHIPA* and its regulation
	Explanation of how ICES' collection and use of PI is permitted under the *Coroners Act* and its regulations
	Explanation of how iCES' collection and use of PI is permitted under the *CYFSA* and its regulations
3. Limitations on ICES Agents	

Initial privacy training must include the following information about limitations on ICES Agents' collection, use, and disclosure of Identifiable Information:	
	Limitations placed on access to and use of Identifiable Information by ICES Agents
	Description of how ICES Agents' activities in the ICES Data Environments are logged, monitored, and audited, including in relation to Identifiable Information
	Limitations, conditions, or restrictions placed on Identifiable Information, including:
	■ Prohibitions on collecting, using, or disclosing Identifiable Information if other information, such as De-Identified Information will serve the identified purposes for collection, use, and disclosure.
	■ Prohibitions on collecting, using, or disclosing more Identifiable Information than is reasonably necessary to servicec the identified purpose
	Description of the procedure to follow if an ICES Agent receives a request to disclose Identifiable Information
4. Privacy Policies, Standards, and Procedures	
Initial privacy training must include the following information about ICES' privacy policies, standards, and procedures:	
	An overview of ICES' privacy policies, standards, and procedures
	An overview of obligations arising from these privacy policies, standards, and procedures
5. Statutory and Compliance Breaches	
Initial privacy training must include the following information about breaches:	
	The consequences of a breach under *PHIPA* or its regulation
	The consequences of a breach under the *Coroners Act* and its regulations
	The consequences of a breach under the *CYFSA* and its regulations
	The consequences of a breach of ICES' privacy policies, standards, and procedures
6. ICES' Privacy Program	

Initial privacy training must include the following information about ICES' privacy program:	
	An explanation of ICES' privacy program, including:
	■ Key activities of the program
	■ The ICES Agent(s) who are delegated day-to-day authority to manage the privacy program
	ICES' administrative, technical, and physical safeguards to protect Identifiable Information against:
	■ Theft, loss, and unauthoriezed collection, use, or disclosure
	■ Copying, modification, or disposal
	The duties and responsibilities of ICES Agents in implementing the administrative, technical, and physical safeguards in place to protect Identifiable Information
7. De-Identified Information	
Initial privacy training must include the following information about De-Identified Information:	
	The purposes that De-Identified Information can be used for
	The purposes that De-Identified Information can be disclosed for
	Prohibition on using De-Identified Information, either alone or with other information, to identify an individual
	The exception to the prohibition of re-identification is if:
	■ The re-identification is done in accordance with ICES' policies, standards, and procedures
	■ The re-identification is permitted under *PHIPA*, the *Coroners Act*, the *CYFSA*, or another applicable law
	■ There is a notice that compliance with this prohibition will be audited and monitored
8. Privacy Notices and Confidentiality Agreements	
Initial privacy training must include the following information about privacy notices and confidentiality agreements:	
	The nature and purpose of privacy notices
	Key provisions of privacy notices
	The nature and purpose of the ICES Agent and Confidentiality Agreement ("ICES Agent CA")
	Key provisions of the ICES Agent CA
9. Privacy Breach Management	

Initial privacy training must include the following information about Privacy Breach management:	
	An explanation of the *Privacy Breach Management Policy*
	An explanation of ICES Agents' duties and responsibilities in identifying, reporting, containing, and participating in the investigation and remediation of Privacy Breaches
	An explanation of an ICES Agent's duty to notify ICES at the first reasonable opportunity of a Privacy Breach or a suspected Privacy Breach
10. Privacy Training	
Initial privacy training must include the following information about privacy training:	
	An explanation that privacy training is mandatory for ICES Agents
	A prohibition on all ICES Agents to handle Identifiable Information without completing initial privacy training
	An explanation that ICES Agents are required to complete ongoing privacy training on an annual basis.
11. Ongoing Privacy Training Requirements	
Ongoing privacy training must include the following information:	
	Role-based training to ensure ICES Agents understand how to apply the privacy policies, standards, and procedures to their responsibilities as they may have evolved since their last training
	Information about new privacy policies, standards, and procedures
	Information about significant amendments to existing policies, standards, and procedures
	Information about relevant changes since the last privacy training, including:
	■ Recommendations with respect to privacy training made in Privacy Impact Assessments, Compliance Audits, and investigations of suspected Privacy Breaches and Privacy Complaints
	■ Orders, decisions, guidelines, fact sheets, and best practices issued by the Information and Privacy Commissioner of Ontario ("IPC") under *PHIPA*, the *Coroners Act*, the *CYFSA*, or their regulations
	■ Amendments to *PHIPA* and its regulation relevant to ICES as a PE
	■ Amendments to the *Coroners Act* and its regulations relevant to ICES as a PE
	■ Amendments to the *CYFSA* and its regulations relevant to ICES as a PE

Appendix B

Initial and Ongoing SecurityTraining - Content Requirements

Initial Security Training
1. An overview of ICES' security policies, standards, and procedures and obligations arising from them.
2. Consequences of breach of:
PHIPA or its regulations (for PHI)
Coroners Act or its regulations (for PI collected by ICES from the Chief Coroner)
CYFSA or its regulations (for PI collected by ICES from Service Providers)
ICES' security policies, standards, and procedures
3. An explanation of ICES' Cybersecurity program, including:
Key activities of the program
The ICES Agent(s) delegated day-to-day authority to manage the Cybersecurity program
4. The administrative, technical, and physical safeguards at ICES to protect Identifiable Information from:
Theft and loss
Unauthorized collection, use, or disclosure
Unauthorized copying, modification, or disposal
5. The duties and responsibilities of ICES Agents in implementing ICES' administrative, technical, and physical safeguards from Identifiable Information.
6. An explanation of the *Security Incident Management Standard* and the *Security Incident Response Plan ("SIRP")*, including:
The duties and responsibilities imposed on ICES Agents in identifying, reporting, containing, and participating in the investigation and remediation of Security Incidents.
The duty of ICES Agents to notify ICES at the first reasonable opportunity of a Security Incident.
7. An explanation of the mandatory nature of security training, including:
The prohibition against ICES Agents accessing and processing Identifiable Information without having completed initial security training
The mandatory requirements to complete security training on an annual basis.
Ongoing Security Training

8. Role-based training so ICES Agents understand how the security policies, standards, and procedures apply to their day-to-day responsibilities.
9. Changes to security policies, standards, and procedures introduced since the previous annual training, including:
    - New security policies, standards, and procedures
    - Significant amendments to existing policies, standards, and procedures
10. Incorporate any relevant changes since the last annual training, including:
    - Security training changes arising from recommendations made in:
        - Privacy Impact Assessments
        - Investigations of Security Incidents
        - Security Audits, including:
            - Threat Risk Assessments
            - Vulnerability assessments
            - Penetration testing/ethical hacks
            - Audits of privacy and information security events
    - Orders, decisions, fact sheets, and best practices issued by the IPC under:
        - *PHIPA* and its regulations
        - *Coroners Act* and its regulations
        - *CYFSA* and its regulations
    - Amendments to:
        - *PHIPA* and its regulations
        - *Coroners Act* and its regulations
        - *CYFSA* and its regulations

Appendix C

Initial and Ongoing Privacy and Security Training – Log Requirements	
At minimum, the log (or combined logs if more than one) of the completion of privacy and security training by ICES Agents must include the following information:	
	1. Name of the ICES Agent
	2. Date of the ICES Agent's commencement of employment or contractual relationship with ICES
	3. Date(s) the initial privacy and security training was completed
	4. Date(s) of subsequent annual completion of privacy and security training