

Privacy and Security Audit Policy



Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	018-00-00	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)
2015-06-01	2025-10-31	Triennial	October 2028	2025-07-31
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal			
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 To ensure the effectiveness of its privacy and security policies, standards, and procedure, ICES' compliance program assesses the adequacy of its controls and compliance with applicable obligations, as detailed in this policy.
- 1.2 ICES' compliance program includes:
 - 1.2.1 **Compliance Audits**, including **In-Depth Audits** and/or **Compliance Reviews**, which are scheduled and conducted in accordance with this policy as well as the following procedures:
 - (a) *Compliance Audit Schedule Procedure*
 - (b) *Compliance Audit Procedure*
 - (c) *Compliance Audits of Agent Access Procedure*
 - 1.2.2 **Security Audits**, which are conducted in accordance with this policy and the *Security Audit Standard*.
- 1.3 Compliance Audit and Security Audit processes demonstrate accountability by ensuring **Department Heads** and the **Executive Team** are properly notified of all audit outcomes.

2.0 SCOPE

- 2.1 This policy applies to all **ICES Agents** and all activities related to **Identifiable Information** collected by ICES and any derivatives of that Identifiable Information.

3.0 ROLES AND RESPONSIBILITIES

- 3.1 Chief Executive Officer ("**CEO**")

Privacy and Security Audit Policy

- 3.1.1 Reviews and approves In-Depth Audits.
- 3.2 Chief Privacy and Legal Officer (“**CPLO**”)
 - 3.2.1 Ensures the schedule of Compliance Audits (“Compliance Audit Schedule”) is developed;
 - 3.2.2 Presents the Compliance Audit Schedule to the Executive Team for approval prior to commencing Compliance Audit activities; and
 - 3.2.3 Presents the “Annual Audit Program Report” to the Executive Team.
- 3.3 Director, Privacy and Legal Office (“**PLO**”)
 - 3.3.1 Oversees Compliance Audit activities;
 - 3.3.2 Reviews and approves the “Annual Audit Program Report” before it is presented to the Executive Team.
- 3.4 Audit **Subject Matter Expert** (“**SME**”)
 - 3.4.1 Leads the development of the Compliance Audit Schedule; and
 - 3.4.2 Prepares the “Annual Audit Program Report”, summarizing the Compliance Audits conducted that year.
- 3.5 Director, Cybersecurity
 - 3.5.1 Implements and oversees Security Audit activities in accordance with the *Security Audit Standard*.
- 3.6 Department Heads
 - 3.6.1 Ensures all activities in the Compliance Audit Schedule relevant to their departments are executed, reported, and actioned in accordance with applicable policies, standards, and procedures.

4.0 DETAILS

- 4.1 Objectives of audit activities
 - 4.1.1 Compliance Audits and Security Audits are conducted to ensure all ICES Agents apply a risk-based approach for demonstrating compliance with regulatory obligations.
 - 4.1.2 Compliance Audits and Security Audits also demonstrate that ICES operates in compliance with applicable obligations, including but not limited to:
 - (a) Obligations relevant to ICES’ role as a **Prescribed Entity** under:
 - (i) *Personal Health Information Protection Act (“PHIPA”)*; and its regulation;
 - (ii) *Coroners Act*, and its regulations;
 - (iii) *Child, Youth and Family Services Act (“CYFSA”)* and its regulations; and
 - (iv) The **IPC Manual**, **Coroners Addendum**, and the **CYFSA Addendum**;
 - (b) Other legislation that ICES relies upon when collecting Identifiable Information;
 - (c) Any insurance policies through ICES’ insurance provider; and
 - (d) Agreements with **Data Providers** and other partners.

Privacy and Security Audit Policy

4.2 Security Audits

4.2.1 Security Audits must be implemented in accordance with the *Security Audit Standard*.

4.3 Compliance Audits

4.3.1 A risk-based approach must be used each year to:

- (a) Prioritize the number and type of Compliance Audits to be conducted in the forthcoming year;
- (b) Enable findings, recommendations, and **Management Action Plans** to be:
 - (i) Managed consistently at the strategic and operational levels of ICES; and
 - (ii) Reported in accordance with the *Compliance Audit Procedure*;
- (c) Ensure credibility and transparency in the auditing process.

4.3.2 Compliance Audits must be conducted by the Audit SME or, if not, in consultation with an Audit SME.

- (a) For In-Depth Audits, the ICES Agent selected to conduct the audit should be sufficiently impartial to the activity under review to ensure objectivity and credibility.

4.3.3 Each year, the Compliance Audit activities cycle through three stages:

- (a) Developing the Compliance Audit Schedule;
- (b) Conducting Compliance Audits; and
- (c) Reporting outcomes of Compliance Audits.

4.4 Developing the Compliance Audit Schedule

4.4.1 A Compliance Audit Schedule must be developed that identifies the Compliance Audits to be conducted during the year. The Compliance Audit Schedule is developed in accordance with the *Compliance Audit Schedule Procedure*.

4.4.2 Development of the Compliance Audit Schedule must be based on a risk-based methodology that takes into account the following factors about the policies, standards, and procedures being considered to audit:

- (i) Maturity;
- (ii) Complexity;
- (iii) History of compliance;
- (iv) Legal and/or regulatory requirements, including recommendations and guidance from the Information and Privacy Commissioner of Ontario ("**IPC**");
- (v) Frequency of use;
- (vi) **Privacy Breaches** and **Security Incidents**;
- (vii) **Privacy Complaints**; and
- (viii) Risk tolerance;

4.4.3 At minimum, the Compliance Audit Schedule must ensure:

Privacy and Security Audit Policy



- (a) The requirements of third parties, such as Data Providers or ICES' insurance provider, are accounted for;
- (b) There is one or more annual audit(s) of ICES Agents access related to:
 - (i) **Personal Health Information (“PHI”)**
 - (ii) **Personal Information (“PI”)**
 - (iii) **Other Identifiable Data**
- (c) There must be one or more annual audit(s) that includes ICES Agent access and/or use to PI, which is initially collected by ICES as a Prescribed Entity under the *Coroners Act* and the *CYFSA*; and
- (d) All privacy and security policies, standards, and procedures are audited at least once every three years.

4.4.4 The Compliance Audit Schedule must include the following information about each Compliance Audit:

- (a) The type of audit;
- (b) The purpose of the audit;
- (c) The scope/nature of the audit; and
- (d) The ICES Agent responsible for conducting the audit.

4.4.5 The Compliance Audit Schedule must be presented to the Executive Team by the CPLO, or their delegate, for approval prior to conducting audit activities.

4.5 Conducting Compliance Audits

4.5.1 Compliance Audits must be conducted and documented in accordance with the *Compliance Audit Procedure* and *Compliance Audits of Agent Access Procedure*.

4.5.2 The process for conducting a Compliance Audit will differ depending on the type of audit being performed (In-Depth Audit or Compliance Review).

4.5.3 All Compliance Audits must include:

- (a) Review of relevant documentation;
- (b) Creation of a plan that sets out appropriate scope, approach, and techniques;
- (c) Notifications to relevant ICES stakeholders;
- (d) Execution through fieldwork;
- (e) Assessment and findings; and
- (f) Communication of findings.

4.6 Risks identified in Compliance Audits

4.6.1 In some instances, there may be risks identified with the findings of a Compliance Audit. Such risks escalated for management through ICES' Enterprise Risk Management (“**ERM**”) program, in accordance with the *Risk Management Policy*.

4.7 Reporting outcomes of Compliance Audits and receiving approvals



Privacy and Security Audit Policy

- 4.7.1 In-Depth Audit Reports must be reviewed and approved by the CEO.
- 4.7.2 An “Annual Audit Program Report” must be prepared that summarizes the Compliance Audits and Security Audits conducted for the year that were included on the Compliance Audit Schedule, and it must include the following information:
 - (a) The findings and recommendations from Compliance Audits;
 - (b) Risks identified with the findings;
 - (c) Associated **Management Action Plans** for recommendations not associated with risks; and
 - (d) Timeframes for implementing these recommendations.
- 4.7.3 The “Annual Audit Program Report” must be presented to the Executive Team by the CPLO, or their delegate, for information purposes.
- 4.8 Logging Compliance Audits
 - 4.8.1 A log of completed Compliance Audits must be maintained and, at minimum, include the information set out in Appendix A.
- 4.9 Suspected Privacy Breaches and Security Incidents identified through Compliance Audits
 - 4.9.1 While conducting audit activities, ICES Agent(s) may identify a suspected Privacy Breach or a Security Incident. In such instances, the ICES Agent(s) must notify ICES at the first reasonable opportunity in accordance with the *Privacy Breach Management Policy* and/or the *Security Incident Management Standard*.

5.0 RELATED DOCUMENTATION

- 5.1 Policies
 - 5.1.1 *Privacy Breach Management Policy*
 - 5.1.2 *Risk Management Policy*
- 5.2 Standards
 - 5.2.1 *Security Incident Management Standard*
 - 5.2.2 *Security Audit Standard*
- 5.3 Procedures
 - 5.3.1 *Compliance Audit Procedure*
 - 5.3.2 *Compliance Audit Schedule Procedure*
 - 5.3.3 *Compliance Audits of Agent Access Procedure*
- 5.4 Tools
- 5.5 Guidelines

6.0 TRAINING AND COMMUNICATION

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

Privacy and Security Audit Policy

- 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**.

Privacy and Security Audit Policy



9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	Change Notes
2025-07-31	<ul style="list-style-type: none">■ Reviewed for compliance with ICES' obligations as a Prescribed Entity:<ul style="list-style-type: none">○ IPC Manual:<ul style="list-style-type: none">▪ 01-27: Policy, Procedures, and Practices in Respect of Privacy Audits▪ 01-28: Log of Privacy Audits▪ 02-18: Policy, Procedures, and Practices in Respect of Information Security Audits○ Coroners Addendum:<ul style="list-style-type: none">▪ 05-28: Policy, Procedures, and Practices in Respect of Privacy Audits▪ 05-29: Log of Privacy Audits▪ Part 2 – Additional Requirements■ Updated to reflect:<ul style="list-style-type: none">○ 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	<ul style="list-style-type: none">■ Revised to reflect the updated ICES Information classification and revisions for overall clarity.

Privacy and Security Audit Policy



Appendix A

Compliance Audits – log requirements	
	At minimum, the log of Compliance Audits must include the following information:
	1. Nature and type of Compliance Audit conducted
	2. Date that the Compliance Audit was completed
	3. The ICES Agent(s) responsible for completing the Compliance Audit
	4. Findings and recommendations, if any, arising from the Compliance Audit
	For any recommendations arising from a Compliance Audit, then the log must also include the following information:
	5. The ICES Agent(s) responsible for addressing the recommendation
	6. The manner in which the recommendation is expected to be addressed
	7. The date the recommendation is expected to be addressed
	8. The manner in which the recommendation was actually addressed
	9. The date the recommendation was actually addressed