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	2025-07-31	Triennial	July 2028	PO.018

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, Procedures, and Practices, ICES has implemented a compliance program, which includes **Compliance Audits** and **Security Audits** to assesses the adequacy of its controls and compliance with applicable obligations, including but not limited to:

1.1.1 The *Personal Health Information Protection Act, 2004 ("PHIPA"),* the *Coroners Act,* their applicable regulations, as well as other legislation relied on to collect, use, or disclose **Personal Health Information ("PHI")** and **Personal Information ("PI")**;

1.1.2 The **IPC Manual** and the **Coroners Addendum**;

1.1.3 Any insurance policies through ICES' insurance provider; and

1.1.4 Agreements with **Data Providers** and other partners.

1.2 Compliance Audits processes demonstrate accountability by ensuring **Department Heads** and the **Executive Team** are properly notified of all Compliance Audit outcomes.

1.3 ICES must conduct scheduled Compliance Audits, including **In-Depth Audits** and/or **Compliance Reviews**, in the manner set out in this Policy, the *Compliance Audit Procedure*, and the *Compliance Audit Schedule Procedure*.

1.4 Security Audits must be implemented in accordance with this Policy and the *Security Audit Standard*.

2.0 SCOPE

2.1 This Policy applies to all **ICES Agents** and activities involving PHI/PI collected by ICES and any derivatives of that PHI/PI.

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Executive Officer (“CEO”)

3.1.1 Accountable for reviewing and approving In-Depth Audits.

3.2 Chief Privacy and Legal Officer (“CPLO”)

3.2.1 Ensures that an **Annual Audit Schedule** is developed;
3.2.2 Presents the Annual Audit Schedule to the Executive Team for approval before any work can proceed; 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 Implements and oversees Compliance Audit activities through the Compliance program;
3.3.2 Supports and leads the development of the Annual Audit Schedule; and
3.3.3 Prepares the “Annual Audit Program Report”, which summarizes all audits conducted throughout the year.

3.4 Director, Cybersecurity

3.4.1 Implements and oversees Security Audit activities, as detailed in the *Security Audit Standard.*

3.5 Department Heads

3.5.1 Ensures that the items in the Annual Audit Schedule relevant to their departments are executed, reported, and actioned in accordance with all applicable Policies, Standards, and Procedures.

4.0 DETAILS

4.1 The objectives of Compliance Audits and Security Audits are to:

4.1.1 Demonstrate that ICES is operating in compliance with section 1.0 of this Policy; and
4.1.2 Ensure all ICES Agents apply a risk-based approach for demonstrating compliance with regulatory obligations:

4.2 Security Audits will be implemented in accordance to the *Security Audit Standard*.
4.3 For Compliance Audits, as set out in the *Compliance Audit Schedule Procedure*, a risk-based approach will be used each year to:

4.3.1 Prioritize the number and type of Compliance Audits to be conducted in the forthcoming year;
4.3.2 Enable findings, recommendations, and **Management Action Plans** to be managed consistently at the strategic and operational levels of ICES and reported as set out in the *Compliance Audit Procedure*; and
4.3.3 Ensure credibility and transparency in the auditing process.

4.4 The ICES Agent selected to conduct any In-Depth Audit should be sufficiently impartial to the activity under review to ensure objectivity and credibility.
4.5 Each year, the Compliance Audit activities will cycle through three stages:

4.5.1 Develop the Annual Audit Schedule;
4.5.2 Execute the Annual Audit Schedule; and
4.5.3 Communicate reports and approvals.

4.6 The Annual Audit Schedule identifies the Compliance Audits to be conducted during the year.

4.6.1 The Annual Audit Schedule must be developed in accordance with the *Compliance Audit Schedule Procedure* and must:

(a) Be based on a risk-based methodology that takes into account the following factors for any Policy, Standard, Procedure, or Practice:

(i) maturity;
(ii) complexity;
(iii) history of compliance;
(iv) legal and/or regulatory requirements and recommendations or guidance from the IPC;

(v) frequency of use;
(vi) **Privacy Breaches** and **Information Security Incidents**;
(vii) **Privacy Complaints**; and
(viii) Risk tolerance;

(b) State the purpose, type, and scope/nature for each Compliance Audit to be conducted, as well as the ICES Agent responsible for conducting the audit;
(c) Account for requirements of third parties, such as ICES' insurance provider or Data Providers;
(d) Adhere to the requirements from the IPC Manual, Coroners Addendum, or other regulatory requirements, including the annual audit of ICES Agents access to PHI/PI; and
(e) Ensure that all privacy and security Policies, Standards, and Procedures are audited at least once every three years.

4.6.2 The Annual Audit Schedule must be presented to the Executive Team for approval before work can proceed.

4.7 When executing the Annual Audit Schedule, all Compliance Audits must be conducted in accordance with the *Compliance Audit Procedure*.

4.7.1 The process for conducting a Compliance Audit will differ depending on the type of audit being performed (In-Depth Audit or Compliance Review).
4.7.2 All Compliance Audits must include:

(a) Review of relevant documentation;

(i) In the course of conducting a Compliance Audit, in-scope documentation may include **Restricted Information** (e.g. PHI/PI) or **Classified Information** (e.g., records from Human Resources, Finance, Data Quality & Information Management, etc.) that cannot be shared with an auditor for personal privacy and/or information security purposes. In these cases, it is permissible for the relevant Department Head to demonstrate compliance either by summarizing the contents of the Classified Information or Restricted Information, or by answering any questions by the auditor about the contents of such information, so long as the Director, PLO is satisfied that sufficient information is provided to adequately conduct the audit.

(b) Creation of a plan that sets out appropriate scope, approach, and techniques;
(c) Notifications;

(d) Execution through fieldwork;
(e) Assessment and findings; and
(f) Communication of findings.

4.8 The findings from each Compliance Audit must be transferred to the **Risk Register** and addressed in accordance with the *Risk Management Policy*.

4.8.1 In-Depth Audit Reports must be reviewed and approved by the CEO.

4.9 Annual Audit Program Report

4.9.1 An "Annual Audit Program Report" must be prepared that sets out a summary of all the Compliance Audits and Security Audits conducted for the year.
4.9.2 The Annual Audit Program Report will include:

(a) The findings and recommendations from Compliance Audits and Security Audits;
(b) Identified risks;
(c) For Compliance Audits, any associated Management Action Plans; and
(d) Timeframes for remediating identified risks.

4.9.3 The Annual Audit Program Report will be presented to the Executive Team by the CPLO for information purposes.

4.10 Escalation

4.10.1 In the course of conducting an audit activity, ICES Agent(s) shall notify ICES at the first reasonable opportunity if:

(a) They identify a suspected Privacy Breach, in accordance with the *Privacy Breach Management* Policy, and/or
(b) They identify an Information Security Incident, in accordance with 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

5.4 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**