Privacy and Security Audit Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.018	ICES Site-Specific Policy	ICES Network	All Acts
Original Date (Month yyyy)	**Last Review Date** (Month yyyy)	**Frequency of review**	**Next Review Due Date** (Month yyyy)	**Supersedes (if applicable)**
June 2014	September 2014	Triennially	September 2025	800PR-PR-007, 800PR-PR-011

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

Required Reviewers (Titles)		
Director, Cybersecurity		

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

1.0 PURPOSE

1.1 To ensure the effectiveness of its privacy and security **Policies**, **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 **Information and Privacy Commissioner of Ontario ("IPC")** *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("**IPC Manual**");

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 ICES **Department Heads** and **Executive Team ("ET")** 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**.

1.4 **Security Audits** must be implemented in accordance with ICES' *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 ICES **Chief Executive Officer** ("**CEO**") is accountable for reviewing and approving **In-Depth Audits.**

3.2 ICES **Chief Privacy and Legal Officer** ("**CPLO**") is responsible for:

3.2.1 Ensuring that an **Annual Audit Schedule** is developed;

3.2.2 Presenting the **Annual Audit Schedule** to the ICES **ET** for approval before any work can proceed; and

3.2.3 Presenting the **Annual Audit Program Report** to the ICES **ET**.

3.3 ICES Director, **Privacy and Legal Office** ("**PLO**") is responsible for:

3.3.1 Implementation and oversight of **Compliance Audit** activities through the ICES compliance program;

3.3.2 Supporting and leading the development of the **Annual Audit Schedule**; and

3.3.3 Preparing the **Annual Audit Program Report,** which summarizes all audits conducted throughout the year.

3.4 ICES Director, Cybersecurity is responsible for:

3.4.1 Implementation and oversight of **Security Audit** activities, as detailed in ICES' *Security Audit Standard*.

3.5 ICES **Department Heads** are responsible for:

3.5.1 Ensuring that the items in the **Annual Audit Schedule** relevant to their departments are executed, reported, and actioned in accordance with all applicable **Policies** 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 ICES' *Security Audit Standard*.

4.3 For **Compliance Audits**, as set out in the *Annual 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 ICES' *Privacy and Security 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 ICES' *Annual Audit Schedule Procedure* and must:

a. Be based on a risk-based methodology that takes into account the following factors for any **Policy**, **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 **Cybersecurity Incidents**;

vii. **Privacy Incidents** or **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 requirements from the **IPC Manual** or other regulatory requirements regarding annual audits of **ICES Agent** access; and

e. Ensure that all privacy and security **Policies** and associated **Procedures** are audited at least once every three years.

4.6.2 The **Annual Audit Schedule** must be presented to the ICES **ET** for approval before work can proceed.

4.7 When executing the **Annual Audit Schedule**, all **Compliance Audits** must be conducted in accordance with ICES' *Privacy and Security 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 **Classified Information** or **Restricted 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 ICES 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 **Corporate Risk Register ("CRR")** and addressed in accordance with ICES' *Risk Management Policy*.

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

4.8.2 Following completion of the **Compliance Audits** planned for the year, an **Annual Audit Program Report** shall be prepared that sets out a summary of all the **Compliance Audits** and **Security Audits** conducted, including the findings and recommendations, identified **Risks**, **Management Action Plans**, and timeframes for remediating identified **Risks**.

4.8.3 The **Annual Audit Program Report** will be presented to the ICES **ET** by the ICES **CPLO** for information purposes.

4.9 Escalation

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

a. They identify a **Cybersecurity Incident** or suspected **Cybersecurity Incident**, in accordance with ICES' *Cybersecurity Incident Management Standard,* and/or

b. They identify a **Privacy Incident**, **Privacy Breach**, or suspect a **Privacy Incident** and/or **Privacy Breach**, in accordance with ICES' *Privacy Incident Breach Management Policy*.

5.0 RELATED DOCUMENTATION

5.1 Policies

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

5.1.2 *Change Management Policy*

5.1.3 *Privacy and Security Audit Policy*

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

5.1.5 *Termination or Cessation of Employment or Contractual Relationship in relation to ICES Data Policy*

5.1.6 *Privacy Incident Breach Management Policy*

5.1.7 *Risk Management Policy*

5.2 Standards

5.2.1 *Cybersecurity Incident Management Standard*

5.2.2 *Security Audit Standard*

5.3 Procedures

5.3.1 *Annual Audit Schedule Procedure*

5.4 Guidelines

5.5 Tools

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 **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** and **Standards** 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, Standards,** 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, Standards,** or **Procedures**, in accordance with ICES' *Privacy Incident Breach Management Policy* and ICES' *Cybersecurity Incident Management Standard*, 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, Standards,** and **Procedures** may be subject to a range of **Disciplinary Actions** in accordance with 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*.

7.4 Compliance is subject to audit in accordance with this **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*.