Privacy Breach Management Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	019-00-00	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)
June 2014	2025-10-31	Triennial	October 2028	2025-07-30
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal Office			
Required Reviewers (Titles)				

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 The purpose of this policy is to create an environment that enables effective detection of and response to:

1.1.1 Suspected **Privacy Breaches**;

1.1.2 Privacy Breaches; and

1.1.3 **Compliance Breaches**.

1.2 This policy also ensures ICES meets its obligations as a **Prescribed Entity ("PE")**, including meeting the requirements set out in:

1.2.1 **IPC Manual**;

1.2.2 **Coroners Addendum**; and

1.2.3 **CYFSA Addendum**.

1.3 When ICES receives a report of a suspected Privacy Breach, an investigation must be opened by Privacy Services to investigate and determine:

1.3.1 Whether a Privacy Breach or Compliance Breach occurred;

1.3.2 If a breach occurred, if it involved Identifiable Information;

1.3.3 The extent of the breach; and

1.3.4 If the breach may also be a **Security Incident**.

2.0 SCOPE

2.1 This policy applies to any suspected Privacy Breach and once investigated, any subsequent findings of a Privacy Breach or a Compliance Breach.

2.2 A Privacy Breach is an occurrence that, at a minimum, includes:

2.2.1 The collection, use, or disclosure of **Identifiable Information** that is not in compliance with law(s) governing the applicable Identifiable Information

2.2.2 Non-compliance with ICES privacy policies, standards, or procedures and the non-compliance is to a provision addressing how Identifiable Information is processed;

2.2.3 Non-compliance with a written agreement where ICES is a named party, and the non-compliance is to a provision addressing how Identifiable Information is processed; and/or

2.2.4 Circumstances where Identifiable Information is stolen, lost or collected, used or disclosed without authority, or where PHI/PI is subject to unauthorized copying, modification or disposal.

2.3 A Compliance Breach is an occurrence that, at minimum, includes:

2.3.1 Non-compliance with ICES policies, standards, or procedures that have an IPC compliance scope; and/or

2.3.2 Non-compliance with a written agreement where ICES is a named party, and the processing of Identifiable Information is contemplated in the agreement.

3.0 ROLES AND RESPONSIBILITIES

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

3.1.1 Approves and oversees establishment of a process for responding to suspected Privacy Breaches, Privacy Breaches, and Compliance Breaches.

3.1.2 Ensures that this process, and all related policies, standards, and procedures, have regard to any guidelines produced by the Information and Privacy Commissioner of Ontario ("**IPC**") relating to Privacy Breaches.

3.2 Director, Privacy and Legal Office ("**PLO**")

3.2.1 Ensures the log tracking suspected Privacy Breaches, Privacy Breaches, and Compliance Breaches adheres to the requirements set out in this policy.

3.3 Privacy **Subject Matter Experts ("SMEs")**

3.3.1 Investigates reported suspected Privacy Breaches and manages Privacy Breaches and Compliance Breaches, in accordance with this policy and the *Privacy Breach Management Procedure.*

3.4 Security SMEs

3.4.1 Manages Security Incidents identified during investigation of a suspected Privacy Breach.

(a) Security Incidents are managed in accordance with the *Security Incident Management Standard*.

3.4.2 Coordinates with Privacy SMEs in investigation, containment, notification, and remediation activities when a Privacy Breach or Compliance Breach is also a Security Incident.

3.5 **ICES Agents**

3.5.1 Reports suspected Privacy Breaches to Privacy Services.

3.5.2 Cooperates during investigation of a suspected Privacy Breach.

3.5.3 Assists the Privacy SME with management of a Privacy Breach or Compliance Breach.

4.0 DETAILS

4.1 Reporting suspected Privacy Breaches

4.1.1 A suspected Privacy Breach is generally identified through:

(a) Notifications from ICES Agents and **Third Party Service Providers** that may or may not be ICES Agents, such as **Electronic Service Providers**;

(b) **Compliance Audits**; and/or

(c) **Privacy Complaints** or **Privacy Inquiries**.

4.1.2 ICES Agents must report a suspected Privacy Breach to Privacy Services at the first reasonable opportunity using one of the following methods:

(a) Emailing privacy@ices.on.ca;

(b) Using the Privacy Services intake form available on the **ICES Intranet**; or

(c) Contacting a member of Privacy Services, either verbally or in writing.

4.1.3 When reporting a suspected Privacy Breach, the ICES Agent must provide the following information:

(a) Their name and contact details (typically email);

(b) Whether the suspected Privacy Breach is at **ICES Central** or, alternatively, the name of the relevant **ICES Site**;

(c) A description of the suspected Privacy Breach;

(d) Whether any **ICES Data** may be impacted, including whether it is Identifiable Information and, to their knowledge, the names of any specific **ICES Data Holdings** (including **ICES Derived Data Holdings**) that may be impacted;

(e) Date (or date range) of the suspect Privacy Breach;

(f) Any steps taken so far as containment measures; and

(g) If applicable, the names of any other individuals who may have further information to support the Privacy SME's investigation into the matter.

4.2 Duty to cooperate

4.2.1 Every ICES Agent has a duty to co-operate with all reasonable inquiries, requests, and instructions from a Privacy SME arising from:

(a) The investigation of a suspected Privacy Breach;

(b) The management of a Privacy Breach; and

(c) The management of a Compliance Breach.

4.2.2 ICES Agents must undertake or assist with reasonable containment efforts, as needed.

4.2.3 ICES Agents must receive approval from Privacy Services or the CPLO prior to notifying any **Data Provider** or other third party about a suspected Privacy Breach.

4.3 Managing suspected Privacy Breaches, confirmed Privacy Breaches, and Compliance Breaches

4.3.1 Upon receipt of an initial report of a suspected Privacy Breach, Privacy Services must promptly initiate the management process to respond to the matter, as further detailed in the *Privacy Breach Management Procedure*.

4.3.2 The CPLO must approve and oversee establishment of the processes for responding to suspected Privacy Breaches, confirmed Privacy Breaches and Compliance Breaches.

4.3.3 The process established by the CPLO must be designed to achieve the following:

(a) Ensure suspected Privacy Breaches are reported to Privacy Services upon detection;

(b) Prompt investigation of suspected Privacy Breaches once reported;

(c) Determine whether a Privacy Breach or Compliance Breach has occurred or no breach has occurred;

(d) Containment of Privacy Breaches and, when necessary, Compliance Breaches;

(e) Notify Data Providers, where required or desirable, at the first reasonable opportunity;

(f) Notify the IPC, where required, in accordance with the IPC Manual and CYFSA Addendum;

(g) Evaluate whether and how to:

(i) Notify other external parties where not required but desirable; and/or

(ii) Provide notice to external parties when requested by the Data Provider;

(h) Fulfill any ICES obligations to co-operate with the IPC, or any other person or organization; and

(i) Identify and address the cause(s) of Privacy Breaches and Compliance Breaches to prevent recurrence.

4.4 Notification obligations

4.4.1 When it is determined appropriate to notify an external party, the CPLO is responsible for:

(a) Making the notification; and

(b) Unless otherwise identified in this policy, the appropriate timeframe for making the notification.

4.4.2 Determination process

(a) The CPLO determines whether to notify external parties about a Privacy Breach or, in more limited circumstances, a Compliance Breach. This determination is made in consultation with the investigating Privacy SME and any other ICES Agents relevant to the investigation process.

(b) Determinations are based on an assessment of the following considerations:

(i) The extent of the Privacy Breach and the nature of the Identifiable Information impacted;

(ii) ICES' existing relationship with the Data Provider;

(iii) ICES' notification obligations as a PE, as set out in more detail below;

(iv) Other applicable legal obligations, including contractual obligations; and

(v) Industry best practices.

4.4.3 Notification to the Data Provider

(a) ICES must notify the Data Provider at the first reasonable opportunity in the following circumstances:

(i) If Identifiable Information has been or is believed to be stolen, lost, or collected, used, or disclosed without authority; or

(ii) If notification is required pursuant to ICES' agreement with the Data Provider.

(b) For **Personal Information ("PI")** collected by ICES as a PE under the *Coroners Act*, ICES must notify the Chief Coroner immediately, in writing, if a **Third Party Researcher** to whom ICES disclosed the PI notifies ICES of a breach.

(c) At minimum, notification to Data Providers, including the Chief Coroner, must be in writing and contain information regarding:

(i) The extent of the Privacy Breach or Compliance Breach;

(ii) The nature of Identifiable Information involved;

(iii) Containment measures implemented; and

(iv) Further actions that ICES will be taking, if any, such as additional investigation and remediation actions.

4.4.4 Notification to the IPC

(a) If the Privacy Breach is regarding **Personal Health Information ("PHI"):**

(i) At the first reasonable opportunity, ICES must notify the IPC in the circumstances set out in subsection 6.3(1) and 18.3(1) of *PHIPA's* regulations, as if ICES was the **Health Information Custodian ("HIC")**.

(b) If the Privacy Breach is regarding PI collected by ICES under the *Child, Youth and Family Services Act ("CYFSA"):*

(i) At the first reasonable opportunity, ICES must notify the IPC in the circumstances set out in subsection 6(3) of the *CYFSA's* regulations, as if ICES were a **Service Provider** (in the context of the *CYFSA*).

(c) Notifications to the IPC must be in writing and include information regarding:

(i) The extent of the Privacy Breach;

(ii) The nature of PHI/PI involved;

(iii) Containment measures implemented; and

(iv) Further actions that ICES will be taking with respect to the Privacy Breach, including investigation and remediation.

4.4.5 Notification to other persons or organizations

(a) Additional notification to other persons or organizations is at the discretion of the CPLO. However ICES should not directly notify individuals whose PHI/PI was impacted by the Privacy Breach.

(i) Unless ICES is informed of an alternative decision approved by the IPC regarding breach notification to affected individuals, notification to those individuals must be provided by the relevant Data Provider who initially collected the PHI/PI from those individuals.

(b) When the CPLO determines it is suitable to notify another person or organization, then notification may be verbal or in writing. The CPLO determines the time frame for these notifications and the information to be included in the notification.

4.5 Logging suspected Privacy Breaches, confirmed Privacy Breaches, and Compliance Breaches

4.5.1 Suspected Privacy Breaches reported to Privacy Services must be logged for tracking, including information regarding the investigation and any related findings of whether Privacy Breaches or Compliance Breaches occurred or if no breach occurred.

4.5.2 At minimum, the **Privacy Breach Log** must include the content set out in Appendix A.

4.5.3 The Director, PLO, is responsible for ensuring the Privacy Breach Log complies with this policy.

4.5.4 The Privacy Breach Log is updated and maintained in accordance with the *Privacy Breach Management Procedure*.

4.6 Relationship to Security Incidents

4.6.1 If a Security Incident is identified during the investigation of a suspected Privacy Breach, then it must also be investigated and managed by a Security SME in accordance with the *Security Incident Management Standard*.

4.6.2 The CPLO has oversight over investigations of both suspected Privacy Breaches and Security Incidents.

4.6.3 Privacy and Security SMEs must coordinate to ensure alignment of their investigation, containment, notification, and remediation activities.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.2 Standards

5.2.1 *Security Incident Management Standard*

5.3 Procedures

5.3.1 *Privacy Breach Management Procedure*

5.4 Tools

5.4.1 Privacy Breach Log

5.4.2 Privacy Services intake form

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 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: ▪ Policies, Procedures, and Practices for Privacy Breach Management ▪ Log of Privacy Breaches ○ Coroners Addendum ▪ Policies, Procedures, and Practices for Privacy Breach Management ▪ Log of Privacy Breaches ○ CYFSA Addendum ▪ Policies, Procedures, and Practices for Privacy Breach Management ▪ Log of Privacy Breaches ■ Updated title from *Privacy Incident and Privacy Breach Management Policy* ■ Added content regarding ICES' role as a Prescribed Entity under CYFSA ■ Revised to reflect updated glossary terms, particularly with regards to Privacy Breaches and Compliance Breaches ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0
2025-10-31	■ Revised to reflect the updated ICES Information classification terminology; additional revisions to improve clarity

Appendix A

Privacy Breach Log Requirements	
At minimum, the log for suspected Privacy Breaches, and confirmed Privacy Breaches and Compliance Breaches, must include the following information:	
	1. The date the suspected Privacy Breach was reported to Privacy Services.
	2. The date the investigation was opened.
	3. The Privacy SME assigned to conduct the investigation.
	4. Who identified the suspected Privacy Breach, including who reported it to Privacy Services if different from who initially identified it.
	5. The date of occurrence of the suspected Privacy Breach.
	6. A description of the suspected Privacy Breach.
	7. If involving ICES Data, the nature of ICES Data impacted, including whether the suspected Privacy Breach involves Personal Health Information (“PHI”), Personal Information (“PI”), or Other Identifiable Data.
	8. The nature and extent of the suspected Privacy Breach or, if confirmed to have occurred, the nature and extent of the Privacy Breach or Compliance Breach.
	9. If notified, the date(s) the Chief Executive Officer (“CEO”) and Executive Team were notified of the suspected Privacy Breach.
	10. The cause of the Privacy Breach or Compliance Breach.
	11. Whether an unauthorized person (someone who is not an ICES Agent or an electronic service provider) caused the Privacy Breach or Compliance Breach, including their name or a description of them.
	12. Containment measures implemented for the Privacy Breach or Compliance Breach.
	13. The date(s) of implementation of containment measures.
	14. The ICES Agent(s) responsible for the containment measures.
	15. The date the investigation was closed.
	16. The findings and recommendations from the investigation.
	Addressing each recommendation arising from an investigation
	17. The ICES Agent(s) responsible for addressing each recommendation
	18. The estimated date that the recommendation is expected to be addressed
	19. The planned manner in which each recommendation is expected to be addressed

	20. The actual date that the recommendation is addressed.
	21. The actual manner in which the recommendation is addressed
If notification is required, or determined appropriate by the CPLO, the log must also include information regarding:	
	22. The date(s) the CEO and Executive Team were notified of the findings and recommendations arising from the investigation.
	23. The date(s) ICES notified impacted Data Providers.
	24. The date that ICES notified the IPC.
	25. The date(s) that ICES notified impacted individuals.