Privacy and Security Incident Breach Management Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.019	ICES Network 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 2022	Triennally	September 2025	N/A

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 The purpose of this **Policy** is to create an environment that enables effective detection of, and response to, **Privacy Breaches** and vulnerabilities that could, if left unaddressed, lead to a **Privacy Breach**.

2.0 SCOPE

2.1 This **Policy** applies to any **Privacy Incident** or **Privacy Breach** that involves **ICES Data**.

2.2 A **Privacy Breach** is any collection, use, disclosure, copying, modification, disposal, loss, theft or other act or failure to act, involving **ICES Data** that is not in accordance with:

2.2.1 Any privacy law.

2.2.2 Any agreement governing ICES' handling of **ICES Data**.

2.2.3 Any ICES **Policy**, **Procedure** or **Practice** (except where previously approved by ICES **Privacy and Legal Office ("PLO")**.

2.3 A **Privacy Breach** also includes circumstances where **ICES Data** is stolen, lost or subject to unauthorized use or disclosure or where **ICES Data** is subject to unauthorized copying, modification, or disposal.

2.4 A Privacy Incident is a suspected Privacy Breach.

3.0 ROLES AND RESPONSIBILITIES

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

3.1.1 Approving and overseeing establishment of a process for responding to **Privacy Incidents** and **Privacy Breaches**.

3.2 ICES Privacy **Subject Matter Experts ("SMEs")**

3.2.1 Managing **Privacy Incidents** and **Privacy Breaches**.

3.3 ICES Cybersecurity Personnel

3.3.1 Managing **Privacy Incidents** and **Privacy Breaches** that are active **Security Incidents**.

3.4 **ICES Employees, ICES Agents, Non-Appointed ICES Agents ("NAIAs"), Collaborating Researchers,** and **Third Party Researchers ("TPRs")**

3.4.1 Reporting **Privacy Incidents** and **Privacy Breaches**, cooperating and assisting with the **Privacy Incident** and **Privacy Breach** management process.

4.0 DETAILS

4.1 Duty to report **Privacy Incidents** and **Privacy Breaches**

4.1.1 Every **ICES Employee, ICES Agent, NAIA, Collaborating Researcher** and **TPR** has a duty to immediately report a **Privacy Incident** or **Privacy Breach** to the ICES **PLO**.

4.2 Responsibility for managing **Privacy Incidents** and **Privacy Breaches**

4.2.1 The ICES **CPLO** is responsible for approving and overseeing establishment of a process for responding to **Privacy Incidents**. This process shall be designed to:

a. Ensure **Privacy Incidents** and **Privacy Breaches** are reported to the ICES **PLO** immediately upon detection;

b. Determine whether a **Privacy Incident** has resulted in a **Privacy Breach**;

c. Contain **Privacy Breaches**;

d. Promptly investigate **Privacy Incidents** and **Privacy Breaches**, once reported;

e. Notify third parties, where required, at the first reasonable opportunity;

f. Evaluate whether and how to notify other parties, and give notice where not required but desirable or requested by a third party;

g. Fulfill any ICES obligations to co-operate with any regulatory authority or other person; and

h. Identify and address the cause(s) of **Privacy Incidents** and **Privacy Breaches** to prevent recurrence.

4.3 Duty to cooperate and assist with management of **Privacy Incidents** and **Privacy Breaches**

4.3.1 Every **ICES Employee, ICES Agent, NAIA, Collaborating Researcher** and **TPR** has a duty to co-operate with all inquiries, requests and instructions from the ICES **PLO** arising from a **Privacy Incident** or **Privacy Breach**. This includes approval of the ICES **PLO** prior to notifying any third party of the **Privacy Breach**.

5.0 RELATED DOCUMENTATION

5.1 Privacy and Security Incident Breach Management Policy

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

5.3 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*

5.4 *Privacy and Security Audit Policy*

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

5.6 *Change Management Policy*

6.0 TRAINING AND COMMUNICATION

6.1 **Policies** and **Procedures** are available on the **ICES Intranet**.

6.2 This **Policy** and any 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 Owner**.

6.3 Once new **Policies** 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** 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** or **Procedures**, in accordance with ICES' *Privacy and Security Incident Breach Management Policy* and associated **Procedures**, 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** and **Procedures** may be subject to a range of **Disciplinary Actions** including warning, temporary or permanent loss of **Access Privileges**, legal sanctions and/or termination of employment for cause, or contract with ICES pursuant to *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* and associated **Procedures**.

7.4 Compliance is subject to annual audit by an ICES Privacy **SME** or ICES Risk & Compliance Analyst pursuant to the **Annual Audit Schedule** established under ICES' *Privacy and Security Audit 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*.