Execution of a section 52.1(1) Agreement Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO		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)**
October 2019	September 2022	Triennially	September 2025	N/A

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

Required Reviewers (Titles)		

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

1.0 PURPOSE

1.1 The purpose of this **Policy** is to identify the circumstances requiring the execution of an agreement by ICES under section 52.1(1) of the *Coroners Act.*

2.0 SCOPE

2.1 This **Policy** applies to the processes and requirements that must be satisfied prior to the execution of a section 52.1(1) agreement.

3.0 ROLES AND RESPONSIBILITIES

4.0 DETAILS

4.1 A section 52.1(1) agreement between ICES and the Chief Coroner must be executed prior to a disclosure of **Personal Information** ("**PI**") by the Chief Coroner to ICES, in accordance with s52.1(1) of the *Coroners Act*.

4.2 ICES **Chief Privacy and Legal Officer ("CPLO")** is responsible for ensuring a section 52.1(1) agreement is executed prior to collection of **PI** from the Chief Coroner.

4.3 Prior to the execution of the agreement, the ICES **CPLO** or delegate of the ICES **Privacy and Legal Office** ("**PLO**") must ensure completion of a **Privacy Impact Assessment** ("**PIA**") that reviews and assesses the legal authority for ICES to collect the **PI** and the Chief Coroner to disclose the information. The requirements for completing the **PIA** are set out in the "ICES **PIA** Form – New Data Holding".

4.4 Once review and assessment of the **PIA** is complete, a copy is provided to the ICES Contracts Specialist and ICES Legal Counsel for drafting of the agreement. The ICES Contracts Specialist must also maintain a log of all section 52.1(1) agreements, which is retained in the ICES PLO's **Contract Management Software** ("**CMS**").

4.5 The ICES **CPLO** must be satisfied the collection of **PI** by ICES is in accordance with ICES' *Collection of ICES Data Policy*.

5.0 RELATED DOCUMENTATION

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

5.2 *Change Management Policy*

5.3 *Privacy and Security Audit Policy*

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

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

5.6 *Privacy and Security Incident Breach 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*.

Execution of a section 52.1(1) Agreement 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*.