Third Party Service Provider Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	005-00-00	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)
2022-09-30	2025-10-31	Triennial	October 2028	2025-07-31

Authority (Title)	Chief Privacy and Legal Officer
Policy Owner (Title)	Director, Privacy and Legal Office
Required Reviewers (Titles)	Director, Cybersecurity
	Director, Research and Analysis

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 This policy provides an overview of how ICES engages **Third Party Service Providers ("TPSPs"),** including principles and requirements that must be met when engaging TPSPs.

1.2 A TPSP is an external person or organization who perform a service or supplies a product to ICES as part of a contractual relationship between ICES and the external person or organization.

1.3 ICES engagements of TPSPs often require ICES to provide access to or share **ICES Confidential Information** with the TPSP. Additionally, some engagements may require ICES to provide access to or share **Restricted Information**, which includes:

1.3.1 **Personal Health Information ("PHI");**

1.3.2 **Personal Information ("PI");** and

1.3.3 **Other Identifiable Data**.

1.4 The requirements and conditions for ICES' engagement of TPSPs will vary depending on the nature of ICES Confidential Information being shared and/or the nature of the services or supplies contemplated in the engagement. Examples include:

1.4.1 Engagements that require access or use of Restricted Information are subject to additional compliance requirements in accordance with the **IPC Manual, Coroners Addendum**, and **CYFSA Addendum**.

1.4.2 ICES' acquisition of goods and services must also be in accordance with the *Procurement Policy*.

2.0 SCOPE

2.1 This policy applies when ICES engages a TPSP, and it applies to the ICES Agents who participate in these processes.

2.2 For clarity, this policy does not apply in the following circumstances:

2.2.1 When ICES acts as an external service provider to a client;

2.2.2 When ICES acts in its capacity as a **Prescribed Entity** under the *Child, Youth and Family Services Act ("**CYFSA**") to* collect PI from **Services Providers** (as defined under the *CYFSA*).

3.0 ROLES AND RESPONSIBILITIES

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

3.1.1 Ensures all TPSPs enter into applicable legal agreements for the circumstances of the engagement and the nature of their services.

3.1.2 Accountable for overall management and tracking of legal agreements between ICES and TPSPs.

3.2 **Sponsor**

3.2.1 Determines how Data Minimization principles are applied when sharing Restricted Information with a TPSP.

3.3 Director, Data Quality and Information Management ("**DQIM**")

3.3.1 Ensures Restricted Information is securely transferred between ICES and a TPSP, in accordance with the applicable agreement.

3.3.2 Documents details regarding transfer of Restricted Information between ICES and a TPSP.

4.0 DETAILS

4.1 Entitlements, authority, duties, and obligations of TPSPs

4.1.1 Entitlements

(a) TPSPs are granted access to **Technology Resources** and ICES Confidential Information in accordance with:

(i) ICES' policies, standards, and procedures; and

(ii) The legal agreement between the ICES and the TPSP.

4.1.2 Authority

(a) When acting on behalf of ICES, TPSPs only have the authority expressly granted to them by ICES during the term of their agency relationship, as set out in the ICES Agent CA or any other legal agreement between ICES and the TPSP regarding the services the TPSP is providing to ICES.

4.1.3 Duties

(a) TPSPs accessing ICES Confidential Information must comply with the *ICES Agent Policy* such that they:

(i) Only engage in activities expressly permitted by ICES' policies, standards, procedures, and applicable legal agreements;

(ii) Not sign documents, or click-to-accept terms and conditions, on behalf of ICES;

(iii) Comply with the restrictions and conditions necessary to enable ICES to comply with its obligations as a Prescribed Entity under *PHIPA*, the *Coroners Act*, and the *CYFSA*.

4.1.4 Obligations

(a) TPSPs must act in accordance with:

(i) ICES' policies, standards, and procedures; and

(ii) Obligations set out in the legal agreement(s) executed between the TPSP and ICES.

(b) TPSPs role as ICES Agents is limited to:

(i) The purposes for which they have been designated an ICES Agent; and

(ii) The duration of their term as an ICES Agent, as set out in the legal agreement between the TPSP and ICES and/or the executed ICES Agent CA.

4.2 Abstractors and ICES Scientists

4.2.1 In addition to any other requirements in this policy, **Abstractors** must comply with ICES' policies, standards, and procedures applicable to their specific role, and any other requirements communicated to them by their Project Manager at ICES.

4.2.2 If an **ICES Scientist** is an ICES Agent and acts in a TPSP capacity for ICES as well, the ICES Scientist must ensure they manage their cross-appointments to avoid actual, perceived, or potential **Conflicts of Interest ("COIs")** in accordance with the *Conflict of Interest Policy*.

4.3 TPSPs as ICES Agents for purposes related to Restricted Information

4.3.1 Subject to exceptions identified in this policy, all TPSPs must be ICES Agents if they are permitted to access and use Restricted Information.

4.3.2 Electronic Service Providers may or may not be ICES Agents. The legal agreement between ICES and an Electronic Service Provider must identify if the Electronic Service Provider will be an ICES Agent when performing services under the legal agreement.

4.3.3 Prior to access to Restricted Information, the following requirements must be met:

(a) A **Privacy Impact Assessment ("PIA")** must be conducted if the contemplated services meet one or more of the criteria set out in the *Privacy Impact Assessment Policy* for when a PIA is required.

(b) A written legal agreement is executed between ICES and the TPSP that meets the requirements of section 4.5 below; and

(c) The TPSP completes privacy and security training in accordance with the *Privacy and Security Training and Awareness Policy.*

4.3.4 TPSPs accessing and using Restricted Information must have vulnerability management practices that meet a standard of protection that is at least equivalent to ICES.

4.4 Data Minimization principles related to Restricted Information

4.4.1 ICES adheres to Data Minimization principles and, as such:

(a) ICES prohibits a TPSP from accessing or using Restricted Information if other information, such as **Sensitive Information**, will serve the purpose; and

(b) ICES prohibits a TPSP from accessing or using more Restricted Information than is reasonably necessary to meet the purpose.

4.4.2 The **Sponsor** of the engagement between ICES and the TPSP determines the necessary amount of Restricted Information to be provided by ICES and, where possible, if other information would serve the purpose instead.

4.4.3 The Sponsor also ensures ICES does not provide more Restricted Information than is reasonably necessary to meet the purpose.

4.5 TPSP agreement requirements related to Restricted Information

4.5.1 When the TPSP will be using Restricted Information (including but not limited to accessing, retention, and disposal of it), ICES must enter into a legal agreement with the TPSP, including Electronic Service Providers, that addresses the information set out in the *Third Party Service Provider Agreement Standard*.

4.5.2 The CPLO is responsible for ensuring all TPSPs enter into applicable legal agreements for the circumstances of the engagement and the nature of their services.

4.5.3 Breach of the agreement between ICES and the TPSP, and steps to address breaches, are subject to the terms of the written agreement between ICES and the TPSP.

4.5.4 ICES Agents must consult Legal Services if there are concerns regarding a possible breach of the agreement by the TPSP or ICES.

4.6 Secure transfer, retention, and disposal of Restricted Information

4.6.1 Restricted Information may be transferred to TPSPs based on ICES acquiring services ICES has determined there is an operational need for, including but not limited to secure back-up for business continuity and disaster recovery, and secure disposal of Restricted Information.

4.6.2 The specific processes and procedures regarding the transfer of the Restricted Information from ICES to the TPSP depends on the nature of the engagement and the terms of the agreement between ICES and the TPSP. At minimum, ICES must ensure the methods used meet the requirements set out in the *Information Handling Standard*.

4.6.3 Secure transfer

(a) The Director, DQIM, or their delegate, is responsible for ensuring Restricted Information is securely transferred between ICES and the TPSP in accordance with the transfer method outlined in the written agreement between them.

(b) Director, DQIM, or their delegate, is responsible for documenting the following details of the transfer:

(A) Date and time of transfer:

(B) Mode of transfer; and

(C) Whether the Restricted Information is transferred for secure retention and/or secure disposal.

(ii) Maintaining a record of the confirmations received from the TPSP upon their receipt of Restricted Information;

(iii) Maintaining a detailed inventory of the Restricted Information being securely retained by the TPSP and of the Restricted Information that ICES has retrieved.

4.6.4 Certificates of Destruction

(a) Tracking of Certificates of Destruction from TPSPs for Restricted Information is handled in accordance with the *Secure Disposal Standard*.

4.7 Management and logging of legal agreements with TPSPs

4.7.1 ICES retains all legal agreements executed between ICES and TPSPs in ICES' contract management software ("**CMS**"). This is completed as part of the processes set out in the *Contract Review Procedure* for executing legal agreements.

4.7.2 For TPSP engagements related to Restricted Information, a log must be maintained that contains the information set out in Appendix A.

4.7.3 The CPLO is accountable for overall management and tracking of these legal agreements. Depending on the nature of the relationship between ICES and the TPSP, day-to-day responsibilities may be delegated to the following departments, as further detailed in the *Contract Review Procedure*:

(a) Legal Services;

(b) Research and Analysis;

(c) Science Office; and

(d) Finance (Procurement).

4.8 Auditing of TPSP engagements related to Restricted Information

4.8.1 ICES may conduct audits on a TPSP's compliance in accordance with:

(a) The terms of the written agreement executed between ICES and the TPSP; and

(b) The *Privacy and Security Audit Policy*.

4.8.2 ICES may or may not notify the TPSP about an audit, subject to the terms of the written agreement between ICES and the TPSP.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Conflict of Interest Policy*

5.1.2 *ICES Agent Policy*

5.1.3 *Privacy and Security Audit Policy*

5.1.4 *Privacy and Security Training and Awareness Policy*

5.1.5 *Privacy Impact Assessment Policy*

5.1.6 *Procurement Policy*

5.2 Standards

5.2.1 *Information Handling Standard*

5.2.2 *Secure Disposal Standard*

5.2.3 *Third Party Service Provider Standard*

5.3 Procedures

5.3.1 *Contract Review 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 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**
2025-07-31	■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ IPC Manual: ▪ 01-19: Policy and procedures for executing agreements with third party service providers in respect of personal health information ▪ 01-20: Template agreement for all third party service providers ▪ 01-21: Log of agreements with third party service providers ○ Coroners Addendum: ▪ 05-20: Policy and procedures for executing agreements with third party service providers in respect of personal information ▪ 05-21: Template agreement for all third party service providers ▪ 05-22: Log of agreements with third party service providers ■ Updated to reflect: ○ Revised glossary terms and titles of ICES policies, standards, and procedures
2025-10-31	Revised to reflect updated ICES Information classification terms; Incorporated CYFSA-related content; and revised for general clarity

Third Party Service Provider Policy

Appendix A

	Third Party Service Provider Agreements – Log Requirements
	At minimum, the log must include the following information regarding agreements between ICES and a TPSP that is permitted to use, including access, to Restricted Information
	1. The name of the TPSP
	2. The nature of the services provided by the TPSP that requires access to and use of Restricted Information
	3. If the TPSP is acting as an ICES Agent or not (i.e. if an Electronic Service Provider that is not an ICES Agent)
	4. The date the agreement was executed by the TPSP and ICES
	5. The date of termination of the agreement between the TPSP and ICES
	If ICES grants the TPSP access to Restricted Information on ICES Data Environments
	6. The date ICES first granted access to the TPSP
	7. The nature of the Restricted Information that the TPSP was granted access to
	8. The date by which ICES must terminate the TPSP's access
	9. The date that ICES terminated the TPSP's access
	If the ICES provides/transfers Restricted Information to the TPSP outside the ICES Data Environments
	10. The date ICES first provided/transferred Restricted Information to the TPSP
	11. The nature of the Restricted Information that was provided/transferred to the TPSP
	12. Whether the Restricted Information will be securely returned by or securely disposed of by the TPSP
	13. The date the Restricted Information must be securely returned by the TPSP, or a Certificate of Destruction must be provided from the TPSP
	14. The date that ICES received the returned Restricted Information or received a Certificate of Destruction from the TPSP