Privacy and Security Governance and Accountability Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	002-00-00	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)
2022-03-01	2025-07-30	Triennial	July 2028	PO.001

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

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 ICES as Prescribed Entity under PHIPA

1.1.1 ICES is a prescribed entity pursuant to the *Personal Health Information Protection Act, 2004* ("*PHIPA*") and its Ontario Regulation 329/04.

1.1.2 *PHIPA* is a consent-based statute in that a **Health Information Custodian" ("HIC")** may collect, use, and disclose **Personal Health Information ("PHI")** only with the consent of the individual to whom the **PHI** relates, subject to limited exceptions where *PHIPA* permits or requires the collection, use, or disclosure to be made without consent.

1.1.3 One such disclosure that is permitted without consent is the disclosure of **PHI** by **HICs** to **Prescribed Entities ("PEs")** for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system.

1.1.4 Disclosures from **HICs** to ICES is permitted without consent provided that ICES has in place policies, standards, and procedures approved and reviewed by the Information and Privacy Commissioner of Ontario ("IPC") every three years from the date of their initial approval.

1.1.5 The review and approval of ICES' policies, standads, and procedures is supported through the application of the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("**IPC Manual**").

1.2 ICES as a Prescribed Entity under the *Coroners Act*

1.2.1 ICES is designated a **Prescribed Entity** under s.2 of Ontario Regulation 523/18 to the *Coroners Act*, for the purposes of s.52.1 of the *Coroners Act* and, as such, ICES has legal authority to collect **Personal Information ("PI")** from the Chief Coroner of Ontario for the purpose of research, data analysis or the compilation of statistical information related to the health or safety of the public, or any segment of the public.

1.2.2 ICES must have in place policies, standards, and procedures approved by the IPC every three years, and this review is supported through the application of the *Coroners Act Addendum to the Manual for the Review and Approval of Persons and Prescribed Entities* ("**Coroners Addendum**").

1.3 ICES as a Prescribed Entity under *CYFSA*

1.3.1 ICES is designated a **Prescribed Entity** under s.1 of Ontario Regulation 191/18 to the *Child, Youth and Family Services Act, 2017* ("*CYFSA*"), for the purposes of s.293 of the *CYFSA* and, as such, ICES has legal authority to collect **PI** from service providers for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, the allocation of resources to or planning for those services, including their delivery.

1.3.2 ICES must have in place policies, standards, and procedures approved by the IPC every three years, and this review is supported through the application of the *Child, Youth and Family Services Act Addendum to the Manual for the Review and Approval of Persons and Prescribed Entities* ("**CYFSA Addendum**").

1.4 As set out in the **IPC Manual**, **Coroners Addendum**, and the **CYFSA Addendum**, to protect the privacy of individuals whose **PHI/PI** is received by ICES and to maintain the confidentiality of that information, ICES must have a *Privacy and Security Governance and Accountability Policy* for ensuring compliance with *PHIPA*, the *Coroners Act*, the *CYFSA*, and their regulations, and for demonstrating compliance with the privacy and security policies, standards, and procedures implemented and operationalized.

1.5 This policy sets out ICES' *Privacy and Security Governance and Accountability Policy* in relation to *PHIPA*, the *Coroners Act*, the *CYFSA*, and their regulations, but also with respect to any other instance in which ICES leverages legal authority under any other statute and/or regulation of Ontario or Canada or its status as a legal not-for-profit corporation duly incorporated in the province of Ontario.

2.0 SCOPE

2.1 This policy applies to ICES and **ICES Agents**.

3.0 ROLES AND RESPONSIBILITIES

3.1 [Currently omitted]

4.0 DETAILS

4.1 Governance

4.1.1 Chief Executive Officer ("CEO") Accountability

(a) The CEO is ultimately accountable for ensuring that ICES and **ICES Agents** comply with *PHIPA*, the *Coroners Act*, the *CYFSA*, their regulations, and with all implemented privacy and security policies, standards, and procedures.

(b) is the CEO is also ultimately accountable for ensuring the security of any **PHI/PI** collected, used, disclosed, transferred, retained and destroyed by ICES and for ensuring that ICES has the resources and technology to implement and execute the security program successfully.

4.1.2 Chief Privacy and Legal Officer ("CPLO") Delegated Accountability

(a) Reporting directly to the CEO, the CPLO is delegated authority from the CEO for executive oversight of the Privacy and Cybersecurity programs.

(b) The CPLO is accountable for the successful execution and implementation of ICES' Privacy and Cybersecurity program in compliance with all regulatory and external requirements.

(c) and the CPLO meets monthly with the CEO and provides a written report regarding the CPLO's accountabilities for the Privacy and Legal Office ("PLO") and the Cybersecurity department.

4.1.3 Board of Directors

(a) The CPLO must provide quarterly written reports to Finance, Audit and Risk Committee ("FAR") Committee of ICES' Board of Directors with regards to the two departments which form part of the CPLO's accountabilities:

(i) PLO functions in each of: Privacy, Legal, Risk, Audit, Compliance; and

(ii) Cybersecurity.

(b) The CPLO attends each FAR meeting, which occur four times per year, and is available to answer questions posed by committee members.

(c) Should the CPLO not be available to attend a FAR meeting, the PLO Director and/or Cybersecurity Director mayattend as delegates, or the CEO may present at the FAR meeting on behalf of the CPLO.

(d) At each quarterly Board of Directors meeting, the Chair of the FAR committee must present the minutes corresponding to the PLO/Cybersecurity written report for formal adoption and approval.

4.1.4 In the PLO/Cybersecurity written report to FAR, the CPLO must (in a level of detail the CPLO deems appropriate) at a minimum provide the FAR committee with information about **Enterprise Risks** that may negatively impact ICES' ability to protect **PHI/PI,** relating to the matters below:

(a) PLO

(i) Major financial investments required to ensure a robust and sustainable privacy governance and accountability framework;

(ii) The development, implementation and evaluation of major information technology transformation projects and high-risk information processing applications with privacy implications, such as artificial intelligence;

(iii) Relevant initiatives undertaken by the PLO, including privacy training;

(iv) The development and implementation of new privacy-related policies, standards, and procedures, including those that are of major, corporate-wide significance and have implications for the Board of Directors, Board members, and the proper functioning of its committees;

(v) The findings and recommendations arising from **Privacy Audits** and **Privacy Impact Assessments ("PIAs")**, including the implementation status of the recommendations;

(vi) **Privacy Breaches** and **Privacy Complaints** that were investigated, as applicable, including the findings and recommendations arising from these investigations and the implementation status of the recommendations;

(vii) Major privacy-related litigation matters, including privacy class-action lawsuits facing ICES;

(viii) Privacy-related issues that have been identified through whistleblowers and/or the *Whistleblower Policy*;

(ix) Major changes to the privacy governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to-day authority to manage the Privacy program and related reporting relationships;

(x) Information about compliance issues, including but not limited to: contractual compliance, regulatory compliance, and the Privacy and Security Audit program; and

(xi) Information regarding **Enterprise Risks** with a corresponding dashboard that also sets out metrics on **Departmental Risks** across the **ICES Network**.

(b) Cybersecurity

(i) Regular updates on the level of cybersecurity risks facing ICES, and the measures that have been put in place to mitigate them;

(ii) Major financial and other investments required to ensure a robust and sustainable information security governance and accountability framework;

(iii) The development, implementation and evaluation of major information technology transformation projects and high-risk information processing applications with information security implications, such as artificial intelligence;

(iv) Relevant initiatives undertaken by the Cybersecurity department, including information security training;

(v) The development and implementation of new information security-related policies, standards, and procedures, including those that are of major, corporate-wide significance and have implications for the Board, Board members and the proper functioning of its committees;

(vi) The findings and associated recommendations arising from information security audits, such as threat and risk assessments, including the status of implementation of recommendations;

(vii) **Information Security Breaches** that were investigated, as applicable, including the findings and recommendations arising from these investigations and the status of implementation of the recommendations;

(viii) Major information security-related litigation matters, including information security class-action lawsuits facing ICES;

(ix) Information-security related issues that have been identified through whistleblowers and/or the *Whistleblower Policy*; and

(x) Major changes to the information security governance and accountability framework, including changes of personnel in high-level position(s) that have been delegated day-to- day authority to manage the information security program and related reporting relationships.

4.2 Roles

4.2.1 Privacy, Risk, and Compliance

(a) Director, PLO

(i) The CPLO has delegated day-to-day responsibility to the Director, PLO for the oversight of the Privacy, Risk, and Compliance programs for ICES;

(ii) The CPLO maintains a current job profile that includes all responsibilities and obligations for the Director, PLO;

(iii) The CPLO meets and reviews the duties and responsibilities of the Director, PLO at least monthly and ensures that any corresponding documentation is kept up-to-date;

(iv) The Director, PLO provides monthly reports to the CPLO on all privacy, risk, and compliance activities;

(v) The Director, PLO has responsibility for the oversight of all Privacy, Risk, and Compliance Analysts ("PRCAs") at each of the **ICES Sites**. Such individuals are not **ICES Employees**, but rather, **Site Employees** of the **Host Institution** with whom ICES has a contractual relationship in respect of an **ICES Site**; and

(vi) The Director, reviews the duties and responsibilities of the PRCAs at least monthly, provides opportunities for regular meetings, and ensures that any corresponding documentation is kept-up-to-date.

(b) Manager, Privacy

(i) The Director, PLO has provided the Manager, Privacy with authority to manage all aspects of the Privacy program for ICES;

(ii) The Director, PLO maintains a current job profile that includes all responsibilities for the Manager, Privacy;

(iii) The Director, PLO meets and reviews the duties and responsibilities of the Manager, Privacy at least monthly and ensures that any corresponding documentation is kept up-to-date;

(iv) The Manager, Privacy provides monthly reports to the Director, PLO on all relevant aspects of ICES' Privacy program within Privacy Services; and

(v) The Manager, Privacy has responsibility to ensure that the Research Program and Project PIA Coordinators, who review **PIAs** for **ICES Projects** utilizing **ICES Data Holdings** categorized as **General Use Data ("GUD")** or **Controlled Use Data ("CUD")** do so in compliance with *PHIPA*, the *Coroners Act*, the *CYFSA*, and their regulations. Research Program and Project PIA Coordinators have a dotted line reporting relationship into the Manager, Privacy for any work related to these **PIAs**.

4.2.2 Cybersecurity

(a) Director, Cybersecurity

(i) The CPLO has delegated day-to-day responsibility to the Director, Cybersecurity for the oversight of the security program for ICES, including but not limited to: strategy development, external stakeholder engagement, and leading large-scale Cybersecurity initiatives and projects;

(ii) The CPLO maintains a current job profile that includes all responsibilities and obligations for the ICE Director, Cybersecurity;

(iii) The CPLO meets and reviews the duties and responsibilities of the Director, Cybersecurity and at least monthly and ensures that any corresponding documentation is kept up-to-date; and

(iv) The Director, Cybersecurity provides monthly reports to the CPLO on all cybersecurity activities.

(b) Manager, Cybersecurity

(i) The Director, Cybersecurity has provided the Manager, Cybersecurity with authority for executing the Cybersecurity department's strategy for ICES, including but not limited to internal stakeholder engagement (departments, teams), leading new processes, policies, tools, forms, logs, identifying and establishing new processes, coordinating tactical and operational changes and remediation activities with Information Technology ("IT") operations and oversight and coordination of complex **Threat Risk Assessments**;

(ii) The Director, Cybersecurity maintains a current job profile that includes all responsibilities for the Manager, Cybersecurity;

(iii) The Director, Cybersecurity meets and reviews the duties and responsibilities of the Manager, Cybersecurity at least monthly and ensures that any corresponding documentation is kept up-to-date; and

(iv) The Manager, Cybersecurity provides monthly reports to the Director, Cybersecurity on all relevant aspects of Cybersecurity security program.

4.3 Privacy and Security Committees

4.3.1 All committees with Privacy and Cybersecurity representation are set out in the *ICES' Governance and Operations Charter*.

4.4 Governance and Organizational Chart

4.4.1 An organizational chart setting out Privacy and Cybersecurity roles is posted on the **ICES Intranet**.

4.5 Privacy and security framework communications to the ICES Network

4.5.1 This **policy** is posted on the **ICES Intranet** and available to all **ICES Agents**.

4.5.2 The CPLO maintains a site on the **ICES Intranet** to update all **ICES Agents** regarding PLO-related and Cybersecurity-related matters, and a more detailed organizational chart is included therein.

4.5.3 Any updates to this *Privacy and Security Governance and Accountability Policy* is communicated at committee meetings, organization-wide eNewsletters and via email announcements, as needed.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Whistleblower Policy*

5.2 Standards

5.3 Procedures

5.4 Tools

5.5 Guidelines

5.6 Other

5.6.1 *ICES Governance and Operations Charter*

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 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: ▪ Privacy Governance and Accountability Framework ▪ Information Security Governance and Accountability Framework ▪ Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program ▪ Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Information Security Program ○ Coroners Addendum: Part 2 – Additional Requirements ○ CYFSA Addendum: Part 2 – Additional Requirements ■ Added content regarding CYFSA ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0

	■ Revised to reflect updated glossary terms and titles of ICES policies, standards, and procedures

=