Protection of Personal Information Policy

1.1 Overview

CPAC's Protection of Personal Information Policy is based upon the ten inter-related principles that form the basis of the CSA Model Code for the Protection of Personal Information outlined in Section 1.4.1 below. These principles lay the framework for information protection best practices across Canadian jurisdictions today, and are intrinsic to all privacy legislation in Canada.

To ensure that CPAC has a fully-realized privacy and security framework, principles and best practices associated with information protection must be understood by all users of personal information. In addition, the principles and best practices must be incorporated into daily practice within the organization. This involves fostering a culture where information protection is seen as a design objective for information and technology – not an obstacle to be overcome. Personal privacy and security of the person are fundamental human rights that are enshrined in legislation worldwide.

This Policy provides management direction to the organization on what needs to be done to protect personal information in CPAC's custody or under its control; it does not specify how the Policy should be implemented. Details associated with how the Policy should be implemented may be found in other components of CPAC's Privacy and Security Framework. CPAC may impose additional direction at its discretion.

1.2 Purpose

The purpose for this policy is to define rules for configuring and managing privacy in a way that protects personal information in CPAC's custody or under its control. The rules:

i. Provide for the lawful collection, use, retention, disclosure, disposition and security of personal information by CPAC.
ii. Facilitate assurance for the public and partners that information protection policies and best practices are being taken into account during the design, implementation and evolution of programs, systems and services within CPAC.
iii. Require the completion of privacy and security assessments, and that privacy and security issues that arise through these assessments are dealt with in a timely manner.
iv. Require that Information Sharing Agreements are completed when personal information is shared with parties that are external to CPAC.
v. Require that records of Information Sharing Agreements, Privacy Impact Assessments and Threat Risk Assessments are managed in a centralized manner in accordance with the level of sensitivity and access requirements.

Through this policy, CPAC can minimize its risks and show due diligence to its partners, stakeholders and the general public.

1.3 Scope

This policy applies to all CPAC employees, consultants and contractors who manage access to and are responsible for the privacy and security of personal information stored in CPAC's information technology assets. It is also applicable to CPAC employees, CPAC Board of Directors, consultants, contractors and partners who handle personal information in any form.

All CPAC employees and members of the CPAC Board of Directors will receive privacy and security awareness training to support their understanding and adherence to this policy.

1.4 Policy Statements

1.4.1. Principles of Information Protection

i. Accountability

Accountability for CPAC's compliance with this Policy rests with the CEO. In practice, the CEO may delegate an individual to act as the Chief Privacy and Security Officer (CPSO).

CPAC will provide privacy and security training in order to support its employees in their efforts to implement the access and release procedures that support this policy.

ii. Identifying Purposes

CPAC shall identify the purposes for which personal information is collected at or before the time the information is collected, and the personal information thus collected shall only be used for the purposes identified to the individual at or before the time it is collected, unless consent is obtained for additional uses and disclosures.

iii. Consent

CPAC shall obtain the consent of the individual for the collection, use and disclosure of personal information, except as authorized by law.

CPAC will use a Knowledgeable Implied Consent model. 'Knowledgeable' means that an individual knows the purpose of a collection, use and/or disclosure, and knows that he or she can give or withhold consent. 'Implied' means that the consent does not have to be express (e.g. communicated to CPAC verbally or in writing) but that CPAC may infer the consent where it is reasonable to do so.

iv. Limiting Collection

CPAC will limit the collection of personal information to what is necessary. Data minimization will be taken into account when designing information systems and business processes.

v. Limiting Use, Disclosure and Retention

Personal information shall only be used or disclosed for the purposes for which it was collected, except with the consent of the individual or as authorized by law.

All information stores shall have retention and destruction schedules.

vi. Accuracy and Integrity

CPAC will have in place for every information store procedures to ensure that personal information is accurate and current.

vii. Safeguards

Personal information collected, used and disclosed by CPAC shall be protected by safeguards appropriate to the sensitivity of the information in order to prevent unintended or unauthorized use, disclosure or deletion.

viii. Openness of Policies, Procedures and Practices

CPAC shall make publicly available specific information about the policies, procedures, and practices relating to the management of personal information. In addition and on request, CPAC may decide at its sole discretion to share general information associated with PIA and TRA outcomes.

ix. Individual Access

CPAC will implement systems and business processes to facilitate access by individuals to their own personal information, and CPAC will similarly provide means for an individual to challenge the accuracy and completeness of the information and amend it as appropriate.

x. Challenging Compliance / Complaints

CPAC encourages interested parties to contact the corporation with any concerns relating to compliance with its own policies and best practices, using the contact information provided. CPAC will investigate and attempt to resolve any complaints and disputes regarding inappropriate collection, use or disclosure of personal information in accordance with the privacy principles and security best practices that form the base for its information protection framework.

1.4.2 Privacy Impact Assessments (PIA)

i. A PIA must be conducted to determine if there are any potential privacy risks associated with a project, program, application, system or new enactment in how it collects, uses, retains or discloses or secures personal information.

ii. A PIA should be conducted by CPAC partners leveraging CPAC IT Systems (e.g. white labelled site) and the results of the PIA must be accepted by CPAC before any service is enabled or program initiated

1.4.3 Threat Risk Assessments (TRA)

i. A TRA should be conducted to identify threats and vulnerabilities associated with the storage and management of information within a project, program, application or system. Any TRA conducted in this regard should clearly identify risks that compromise personal information.

1.4.4 Partner Agreements

i. Where applicable and as required, CPAC must develop Information Sharing Agreements with third parties for the sole purpose of addressing protection of privacy and security of personal information that is exchanged between the parties. This would include information stored in CPAC IT systems or information stored in partner systems in other provinces. The agreements can be separate documents or sections within other agreements.

ii. CPAC must review existing information sharing and partner agreement summaries at least annually.

1.5 Enforcement

Failure to comply with this policy may result in actions which include but are not limited to the following:

i. Denial of access to CPAC information and information technology assets.

ii. Contractual remedies, as may be appropriate for third party suppliers, consultants and/or contractors, such as provisions for breach or termination of contract.

iii. Disciplinary action for employees, including, but not limited to, written warnings, suspensions with or without pay, and/or immediate termination of employment; and/or Prosecution under law.

1.6 Definitions

Term	Definition
Access	The right of an individual or their authorized representative to obtain personal information about themselves from CPAC.
Accountability	An organization is responsible for personal information under its control and shall designate individual(s) who are accountable for the organization's compliance with the CSA Model Code for the Protection of Personal Information, its own policies, and applicable legislation.
Accuracy	The recording of statements of facts, opinions, determinations or assessments that reflect as near as possible what has been provided by the individual, and what the collector has ascertained, hypothesized or determined to be true.
Consent	There must be voluntary agreement of the data subject to the collection, use, and disclosure of his/her personal information. This consent may be either expressed or implied, and should include an explanation as to the implications of withdrawing consent.

	Expressed consent is given explicitly and unambiguously, either verbally or in writing. It is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent is given when the action/inaction of an individual reasonably infers this consent. Consent should never be a condition for supplying a product or service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose.
Control of Information	Information that is in CPAC's custody (see definition immediately below), and that is collected, acquired, updated, deleted, used and disclosed at CPAC's discretion and within the boundaries of the law.
Custody of Information	Information that is being kept or stored by CPAC in its offices, facilities, file cabinets or computers.
Disclosure	To release or make available personal information to a person other than the person the information concerns or a person employed by, or in the service of, the person or organization holding the information.

Personal Information	Recorded information about an identifiable individual, including: • Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual. • Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved. • Any identifying number, symbol or other particular assigned to the individual. • The address, telephone number, fingerprints or blood type of the individual. • The personal opinions or views of the individual except where they relate to another individual. • Correspondence sent to CPAC by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence. • The views or opinions of another individual about the individual. • The individual's name where it appears with other personal information Relating to the individual or where the disclosure of the name would reveal other personal information about the individual. Identifiable information is any data that uniquely links an individual to other piece(s) of data. Examples include PINs (personal identification numbers), access cards, passwords, retinal and fingerprint scans, and e-mail or IP addresses. This type of information should be treated in the same manner as personal information collected in an 'offline' environment.
Privacy	The right of an individual to control the collection, use, and disclosure of personal information about himself or herself.
Safeguards	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
Use	Use refers to the treatment and handling of personal information within an organization.
Collection	The process of gathering or obtaining personal information. Information can be collected directly from a client or indirectly, such as from an individual's legally authorized representative or custodian.
Security	The means by which data/information is protected from accidental or malicious disclosure, modification, removal, or destruction.

Information and Information Technology Assets	Computer equipment (including laptop and desktop computers), software, operating systems, storage media, network accounts, electronic mail, internet access, portals, gateways, network devices, mobile devices, servers, telephones and telephone systems, multifunction printers, personal/home computers while they are connected to the CPAC network either directly or over a VPN connection, information assets (whatever the media or format type) such as business or personal information, and any other thing that may be considered by CPAC to be an information and information technology asset.
Privacy and Security Framework	All policies, standards, tools, templates, processes and procedures that individually and collectively govern the privacy and security of CPAC's information and information technology assets.

Related Documents

- Information Management Policy
- Records Management Policy
- Information and Information Technology (I&IT) Security Policy
- Information Classification Policy
- Access and Release of Personal Information Policy
- Access and Release of Personal Information Procedures
- Acceptable Use Policy
- Privacy Impact Assessment Template
- Threat Risk Assessment Template
- Data Sharing Agreement Template

End of Document