Acceptable Use Policy

1.1 Overview

An Acceptable Use Policy is an integral part of CPAC's Privacy and Security Framework. CPAC has adopted a philosophy of self-regulation and offers users access to its information and information technology (IT) assets provided that the users accept personal responsibility for actions taken when accessing and using the assets. CPAC will not provide a warning system should the user contravene this policy; it is up to the user to know when his/her actions are in violation of the policy.

This Policy provides management direction to the organization on what uses of CPAC's IT assets are acceptable (or unacceptable); it does not specify how the Policy should be implemented. Details associated with how the Policy should be implemented can 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 of this document is to establish acceptable and unacceptable uses for CPAC's IT assets, thereby enabling CPAC as an organization to demonstrate accountability for its actions. All CPAC employees will receive privacy and security awareness training to support their understanding and adherence to this policy.

1.3 Scope

This policy applies to all CPAC employees, consultants, contractors and partners who use CPAC's IT assets.

1.4 Policy Statements

1.4.1 Accountability

i. Each Director and VP are accountable for addressing inappropriate access or use of CPAC's assets by any user working for their business area.
ii. Users of CPAC's IT assets must safeguard all physical and logical assets with which they have been entrusted.

1.4.2 Acceptable Uses

i. Users are permitted to use CPAC's IT assets for business activities that are specifically related to their job function in support of CPAC's strategies and objectives.

ii. Limited personal use of CPAC's IT assets is acceptable as long as the use do not violate CPAC's Privacy and Security Framework, or interfere with a user's delivery of work. Users are responsible for exercising good judgment regarding the reasonableness of personal uses of CPAC's IT assets.

1.4.3 Unacceptable Uses

i. It is unacceptable to use CPAC's IT assets for any illegal purpose, including but not limited to:
- Breaching legal protection provided by copyright and/or license to computer programs, technology or information.
- Breaching privacy and/or security protections described in the Criminal Code of Canada.
- Breaching privacy and/or security protections described in any other statutory instruments that CPAC is or may be governed by.
- Breaching legal protection provided by sexual harassment or hostile workplace laws.

ii. It is unacceptable to use CPAC's IT assets to engage in any behaviour that may jeopardize or be in violation of CPAC's Privacy and Security Framework, including but not limited to:
- Wilfully bypassing or subverting CPAC's physical electronic or procedural security controls.
- Attempting to alter or destroy CPAC IT assets (e.g. information, networks and electronics).
- Deliberately propagating malicious code (e.g. viruses, worms, Trojans or malware).
- Wilfully accessing information that is not required as part of a user's job function.
- Allowing unauthorized individuals to use or access CPAC's IT assets.
- Using unapproved peer-to-peer networking for personal use.
- Installing pirated or other software products that are not licensed for use by CPAC.
- Plagiarizing another CPAC user's work (which may constitute 'intellectual property').
- Engaging in activities that can be considered to disrupt network communications, such as network sniffing, ping floods, packet spoofing, denial of service, and forged routing of information.
- Accessing, using or disclosing personal information without the explicit consent of the individual to whom the information relates (except as required by law).

- Accessing, using or disclosing confidential or restricted information without CPAC's authorization to do so.
- Circumventing user authentication or security of CPAC's IT assets.

iii. It is unacceptable to use CPAC's IT assets in any way that would contravene CPAC's Respect in the Workplace Policy. For example, users must not engage in generating or transmitting unsolicited commercial or advertising material such as spam or chain mail, or harassing or inappropriate materials. In addition, users must not engage in generating or transmitting threats of violence.

iv. It is unacceptable to use CPAC's IT assets for personal gain (e.g. conducting commercial business).

v. It is unacceptable to send anonymous messages in contradiction with CPAC's transparency and accountability core values.

vi. It is unacceptable to purposely access or view inappropriate content on the internet, such as websites that promote hate, that offer pornography or to participate in electronic gambling. CPAC acknowledges that accidental access is possible, and it has the ability to ascertain the difference between purposeful or accidental access.

vii. Social networking (blogging, wikis, instant messaging, Skype, Facebook, Twitter etc.) must be done in a professional, transparent and responsible manner, and personal use must not interfere with a user's regular work duties. In addition, social networking must not be done in a way that is detrimental to CPAC's best interests.

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's 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 for cause without notice or other obligation.

1.6 Definitions

Term	Definition
Information Assets 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.
User	Any person who accesses and uses CPAC's information and information technology assets.

1.7 Related Documents

- Protection of Personal Information Policy
- Information and Information Technology (I&IT) Security Policy
- Information Management Policy
- Records Management Policy
- Respect in the Workplace Policy
- Information Classification Policy
- Password Standard
- Encryption Standard
- Electronic Mail Standard
- Audit and Vulnerability Management Standard
- Access and Release of Personal Information Procedures

End of document