CANADIAN PARTNERSHIP AGAINST CANCER

PARTENARIAT CANADIEN CONTRE LE CANCER

ACCEPTABLE USE POLICY

As of May 2020

POLICY PURPOSE

The **Acceptable Use Policy** provides a framework for the responsible and accepted use of CPAC's information technology resources (such as: hosted, cloud, and local infrastructure, network services, computers, mobiles, applications, networks, software, communications, and databases).

Our technology and cloud solutions support CPAC's business, and include cybersecurity solutions supporting our regulatory, legal, and cybersecurity programs and obligations.

As a user of CPAC's information systems, your use is to support this purpose; any other use of our information technology is secondary and not business-related.

All users have a reasonable expectation of privacy and fair access to information technology resources. However, when using corporate resources, CPAC's cybersecurity monitoring and logging may capture activity and traffic across its networks, cloud providers, and devices. For further information regarding user expectations of privacy, and how CPAC uses and safeguards data and Personal Information please refer to the **Employee Privacy Policy.**

Prohibited activities that jeopardize the integrity, unfair consumption, privacy and safety of others will not be tolerated. Violations of this policy are handled as indicated by Talent Management for employees, and by Partner & Vendor Services for contract work.

AUDIENCE

All CPAC employees, contractors and 3rd parties with trusted access to CPAC information or technology systems.

PRINCIPLES

1. CPAC's information and information technology resources are valuable assets that require responsible care and diligence to prevent abuse, theft, and Cybersecurity Incidents.

2. Limiting access to and use of CPAC information and technology resources can mitigate the risk of Cybersecurity Incidents and prevent the use of CPAC information and technology resources for inappropriate purposes. Information Technology controls may limit your access for this intention.

3. Mobile Computing Devices (which connect to the CPAC Systems and Services, such as mobile phones, tablets, laptops, and other connected devices), removable media (such as USB drives), and employee-owned Devices used for CPAC business purposes must

comply with the acceptable use policy. This may include mobile device management technologies.

4. Cloud and Outsourced Vendor Technology solutions are subject to approval by the Director, Information Technology prior to implementation and must also comply with the acceptable use policy.

ROLE OF EXECUTIVE COMMITTEE

To receive, review and adopt this policy and any recommended amendments thereto.

1. DEFINITIONS

1.01 Authorized Users- individuals who have been authorized to connect to CPAC Systems and Services and includes remote access and/or third-party users approved by the appropriate CPAC authority.

1.02 CASL – An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23.

1.03 CPAC Systems and Services – all the networks, technical infrastructure, applications and end user technology that is connected, owned and/or operated by CPAC.

1.04 Cloud – information technology services offered where the location of the computing infrastructure is not located in CPAC's facilities.

1.05 Cybersecurity - a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

1.06 Outsourced Vendor Technology - any information technology service not provided by CPAC.

1.07 Device – any item, including personally owned, CPAC-owned and publicly owned, capable of connecting to the CPAC Systems and Services, including mobile phones, tablets and laptops.

1.08 Electronic Communications – communications including messaging, voice, Internet browsing logs, audit logs, video, email and other documents created, sent or received using the CPAC Systems and Services.

1.09 Cybersecurity Incident – includes attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data, and changes to system hardware, firmware, or software characteristics without CPAC's knowledge, instruction, or consent.

1.10 Network Data – any data created, received or sent using the CPAC Systems and Services.

1.11 Personal Information - information about an identifiable individual or as information that allows an individual to be identified whether it is recorded or not.

1.12 IT – Information Technology.

1.13 Third-Party Service Provider – any third party offering a service that may affect the CPAC Systems and Services.

1.14 Unauthorized Content - material that intimidates, threatens, humiliates or discriminates against any individual or group; pornographic content; defamatory references or depictions.

1.15 Unauthorized Activities - sending or posting discriminatory, harassing, or threatening messages or images; perpetrating any form of fraud or theft; using, or disclosing someone else's password without authorization; downloading, copying or pirating software, film, music or electronic files that are copyrighted without authorization; sharing confidential material, trade secrets, or proprietary information outside of the organization without authorization; accessing unauthorized websites; sending, posting or intentionally accessing information that is defamatory to CPAC, its products/services, colleagues or customers; introducing malicious software onto the CPAC Systems and Services; jeopardizing the Cybersecurity of CPAC Systems and Services; sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities without authorization.

ACCEPTABLE USE POLICY

2. RESPONSIBILITIES

2.01 CPAC Executive Committee

(a) Receive, review and adopt this policy and any recommended amendments thereto.

(b) Review and adopt procedures which are developed for the implementation of this policy.

(c) Monitor the application, interpretation and administration of this policy.

2.02 Director, Information Technology

(a) Ensure that other Directors and Managers manage the authorized use the CPAC Systems and Services in their respective departments.

(b) Ensure that all employees and third parties have had the opportunity to read this policy and obtain clarification on this policy.

(c) Implementing, reviewing and monitoring supporting Cybersecurity standards such as password, remote access, and mobile devices.

(d) issuing and monitoring compliance with this policy.

(e) Ensure that this policy is reviewed periodically and updated when required.

2.03 Directors and Managers

(a) Determine which of their employees and third parties operating in their division are required to be Authorized Users.

(b) Determine which CPAC Systems and Services and Devices each of their employees and third parties operating in their division will be authorized to access.

(c) Ensure that all employees and third parties operating in their division who are Authorized Users have had the opportunity to read this policy and obtain clarification on this policy.

(d) In the case of violations to this policy, pursue the appropriate disciplinary action with Talent Management.

(e) Implementing, reviewing and monitoring, as well as ensuring compliance with the applicable Standards outlined in the Cybersecurity Manual.

2.04 Talent Management

(a) Handling instances of non-compliance or violations of this Policy and the acceptable use of CPAC's information technology resources.

(b) Escalating violations of this Policy or the acceptable use of CPAC's information technology resources to the Director of Information Technology where required.

(c) Assist in the delivery of E-Learning solutions to CPAC employees.

2.05 Information Technology Employees

(a) Provide information security awareness training tools and solutions.

(b) Employ technology systems, activity logs, performance analyzers, data recovery and archival tools, monitoring and filtering tools, and visual confirmation as cybersecurity incident detection and prevention tools.

(c) Assess and approve software or hardware for use on, or connecting with, the CPAC Systems and Services.

(d) Provide CPAC Systems and Services usage/audit information as requested and required to Talent Management.

(e) Implementing, reviewing and monitoring, as well as ensuring compliance with the appropriate information security Standards outlined in the Cybersecurity Manual.

2.06 All Employees, Contractors and Authorized Users

(a) Shall adhere to the requirements of this Acceptable Use Policy and the applicable information security Standards outlined in the Cybersecurity Manual.

(b) Use CPAC Systems and Services in a responsible, ethical, law-abiding manner.

(c) Acknowledge that CPAC may monitor CPAC Systems and Services, and Devices.

(d) Understand that Electronic Communications pursuant to employment and/or a contract with CPAC are considered CPAC's property.

(e) Make use of CPAC's resources and training in Cybersecurity and make informed, security-conscious decisions.

(f) Report suspected Cybersecurity breaches or potential Cybersecurity Incidents to their immediate supervisor and the IT Service Manager.

(g) Protect CPAC information, such as account credentials, passwords, electronic information, and other information assets in regard to using CPAC Systems and Services.

(h) Consult with Information Technology Employees for Cybersecurity guidance in any circumstance.

(i) Understand that employees may engage in limited personal use of CPAC information technology, in accordance with this policy and its standards, but that all CPAC data may be monitored and personal use must not impact the functioning of CPAC Systems and Services.

3. PROHIBITED ACTIVITIES

3.01 Users are responsible for respecting the privacy of others and for protecting their corporate identity and information access. Users are also responsible for properly using technology resources and avoiding activities that would have a negative effective on others. Using the CPAC Systems and Services for the following purposes is considered a violation of this policy:

(a) Intentionally accessing any Unauthorized Content or performing any Unauthorized Activities.
(b) Conducting business activities unrelated to CPAC employment or contract for personal gain.
(c) Unauthorized access use or disclosure of personal information, confidential information, or proprietary data belonging to CPAC or another person or entity with whom CPAC conducts business.
(d) Accessing or attempting to access another user's account or Cloud service account without authorization.
(e) Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access.
(f) Installing unlicensed or unauthorized content.
(g) Using the CPAC Systems and Services to breach any international, federal, provincial or local law, including intellectual property laws and CASL.
(h) Using CPAC information technologies to originate, store or disseminate materials that harasses, intimidates or threatens individuals or groups.
(i) Connecting any Device that is not owned by CPAC to the CPAC Systems and Services without authorization.
(j) Compromising the Cybersecurity of the CPAC Systems and Services.
(k) Using CPAC IT assets in a way that degrades the performance of the CPAC Systems and Services.

(l) Attempting to remove or alter network and or device safeguards installed on CPAC Systems and Services.
(m) Sending anonymous messages in contradiction with CPAC's transparency and accountability core values.

ENFORCEMENT AND IMPLEMENTATION

Each manager is responsible for implementing, reviewing and monitoring the acceptable usage and employee privacy policy and to assure compliance with this standard.

Non-compliance with this policy will be investigated and action may be recommended in accordance with CPAC Talent Management and the Director, Information Technology.

Exceptions: There are very few, if any situations where an exception will be granted to this policy. All exceptions must be approved by the Director, Information Technology.

This policy shall supersede all previous CPAC Acceptable Usage policies. This policy may be amended or revised at any time. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions.

Appendix A – Acceptable Use Policy Employee/Contractor Sign-Off

I acknowledge that I have read the Canadian Partnership Against Cancer's Acceptable Use Policy and understand my obligations as an employee to comply with the policies outlined in this Policy. I understand that this access is being provided for business purposes only, and subject to any exceptions to this Policy herein. I understand that CPAC cannot restrict access to all controversial and inappropriate materials and I will not hold it responsible for materials acquired on the network.

Finally, I understand that violation of this policy may have consequences ranging from revocation of access privileges to suspension or termination and that CPAC reserves the right to report any unlawful activity to law enforcement and to cooperate in any investigation of such activity.

CPAC does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of employment, or the direct consequence of the discharge of the employee's or contractor's duties. Accordingly, to the extent permitted by law, CPAC reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Dated this _____ day of _____, 20__

Employee/Contractor's Name: _____

Employee/Contractor's Signature: _____