	<b>Remote Access Standard</b>	
	<b>Effective date:</b> April 12, 2013 <b>Policy owner:</b> Chief Privacy & Security Officer <b>Last Revised Date:</b> November 2016 <b>Next Review:</b> 2018 <b>Contact:</b> Director, Information Technology <b>Approved by:</b> Strategic Management Committee	Page 1 of 5

## Remote Access Standard

### 1.1 Overview

CPAC is committed to protecting employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective Remote Access security is an effort involving the participation and support of every CPAC employee and affiliate who accesses CPAC information and information technology assets remotely as part of their role.

To ensure that CPAC's information and information technology remains secured appropriately, effective remote access controls are defined in this document. CPAC may impose more stringent direction at its discretion.

### 1.2 Purpose


The purpose of this document is to provide a set of minimum privacy and security standards (hereinafter called 'the Standard') to be implemented for remote access.

### 1.3 Scope


This standard is mandatory and applies to all CPAC employees, consultants and contractors who manage, set up, and/or administer remote access within CPAC. It also applies to those employees, consultants and contractors who connect to CPAC's information systems with any device from a location outside of CPAC's 1 University Office.

### 1.4 Standards

- i. All CPAC policies and standards remain in force, when CPAC information and information technology assets are accessed remotely. Users must read and understand all CPAC policies and standards that apply to them, particularly those listed at the end of this document.
- ii. Users may access CPAC information and information technology assets using assigned credentials only.

	<b>Remote Access Standard</b>	
	<b>Effective date:</b> April 12, 2013 <b>Policy owner:</b> Chief Privacy & Security Officer <b>Last Revised Date:</b> November 2016 <b>Next Review:</b> November 2017 <b>Contact:</b> Director, Information Technology <b>Approved by:</b> Strategic Management Committee	Page 2 of 5

- iii. Users are strictly forbidden to store any CPAC confidential or restricted information on home/remote computers with the exception of temporarily saving information to conduct work at home. Users should refer to the Information Classification Policy for definitions of confidential and restricted information.
- iv. As an added security measure, remote access to restricted information is only permitted using two-factor authentication.
- v. Users must ensure that the device being used to remotely connect to CPAC's information and information technology assets is not connected to any other network at the same time, with the exception of home computer networks that are under the complete control of the user.
- vi. All computers used to access CPAC information and information technology assets remotely must be secured and maintained as prescribed below:
  - Antivirus, Anti-spyware/malware and Firewall measures must be installed and configured to protect information on the computer.
  - Software updates or patches must be installed and kept up to date.
  - Ensure that CPAC information is not automatically backed up to the cloud.
- vii. Where two-factor authentication is required, CPAC uses an Out of Band system which sends one-time passwords to a user's mobile phone. Users of two-factor authentication are required to:
  - Never disclose one-time passwords to any other user
  - Never copy one-time passwords to any type of media
- viii. Remote access to CPAC information and information technology assets via a home wireless network is permitted where appropriate security measures are applied. Minimally, these measures are:
  - Wireless routers must be configured to use either the WPA or WPA2 encryption protocols.

	<b>Remote Access Standard</b>	
	<b>Effective date:</b> April 12, 2013 <b>Policy owner:</b> Chief Privacy & Security Officer <b>Last Revised Date:</b> November 2016 <b>Next Review:</b> November 2017 <b>Contact:</b> Director, Information Technology <b>Approved by:</b> Strategic Management Committee	Page 3 of 5

- The SSID (WiFi Network Broadcast Name) should be configured so that it does not contain any identifying information about CPAC or the employee, such as the company name, employee name, or address.
  - The wireless password is not configured to be easily guessed and known only to authorized users.
  - New connections are not allowed without the explicit approval of the administrator/owner of the wireless network.
- ix. Remote access to CPAC information and information technology assets via public wireless/WiFi networks is only permitted using CPAC approved secure VPN. This includes access from locations such as Cafes and other publically broadcasting and untrusted WiFi networks. Remote access to CPAC information and information technology assets from mobile devices is only permitted via cellular data and never via public wireless/WiFi networks.

## 1.5 Enforcement

Failure to comply with this standard 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
<b>Information Assets and Information Technology Assets</b>	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.
<b>User</b>	Any person who accesses and uses CPAC resources.
<b>Remote Access</b>	Accessing CPAC Systems from locations other than the premises of CPAC.
<b>Two-factor authentication</b>	Two-factor authentication requires two independent factors before access is authorized (e.g. something that is held by an authorized person, and something that is known to an authorized person). Two-factor authentication typically includes: <ul style="list-style-type: none"> <li>• A valid username and password, issued by CPAC to an individual.</li> <li>• A pin/password sent to an individual's mobile device via SMS message for the purpose of accessing designated CPAC information.</li> </ul>
<b>Out-of-band authentication</b>	Out of band authentication (OOBA) is a term for a process where authentication requires two different signals from two different networks or channels. The essential idea behind out-of-band authentication is that by using two different channels, authentication systems can guard against fraudulent users that may only have access to one of these channels.

## 1.7 Related Documents

- [Acceptable Use Policy](#)
- [Mobile Device Policy](#)
- [Information and Information Technology \(I&IT\) Security Policy](#)

 <p>CANADIAN PARTNERSHIP AGAINST CANCER</p> <p>PARTENARIAT CANADIEN CONTRE LE CANCER</p>	<b>Remote Access Standard</b>	
	<p><b>Effective date:</b> April 12, 2013  <b>Policy owner:</b> Chief Privacy &amp; Security Officer  <b>Last Revised Date:</b> November 2016  <b>Next Review:</b> November 2017  <b>Contact:</b> Director, Information Technology  <b>Approved by:</b> Strategic Management Committee</p>	<p>Page 5 of 5</p>

- 
- [Information Classification Policy](#)
  - [Electronic Mail Standard](#)
  - [Password Standard](#)
  - [HR Code of Conduct](#)

End of Document