 <p>CANADIAN PARTNERSHIP AGAINST CANCER</p> <p>PARTENARIAT CANADIEN CONTRE LE CANCER</p>	Information Classification Policy	
	<p>Effective date: January 15, 2013 Policy owner: Chief Privacy & Security Officer Last Revised Date: July 2014 Next Review: 2018 Contact: Director, Information Technology Approved by: Strategic Management Committee</p>	Page 1 of 7

Information Classification Policy

1.1 Overview

Information classification is integral part of CPAC’s Privacy and Security Framework. When developing strategies for storing, securing and managing information from inception through archive to destruction, it is essential to understand the value of and separate sensitive information from non-sensitive information. In so doing, privacy and security controls can then be applied that are appropriate and proportional to the sensitivity of the information.

Information Classification is a *process* that groups information assets into categories based upon sensitivity characteristics. The classification process utilizes the sensitivity characteristics to group information into defined classes and associated impacts from compromise and/or modification.

To ensure that information is protected according to its level of sensitivity, classes of information are defined in this document. CPAC may impose additional classifications at its discretion.

1.2 Purpose


The purpose of this document is to provide guidance on information classification and handling, along with information classes that form part of CPAC’s Privacy and Security Framework. 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 and contractors who handle information in CPAC’s custody or under its control, and/or who apply privacy and security controls to CPAC’s information technology assets.

1.4 Policy Statements

- i. In order to protect information according to level of sensitivity, it is necessary to identify information assets, and to apply a value to the assets in the context of confidentiality, integrity and availability. For this, CPAC leverages information classification standards from

 <p>CANADIAN PARTNERSHIP AGAINST CANCER</p> <p>PARTENARIAT CANADIEN CONTRE LE CANCER</p>	Information Classification Policy	
	<p>Effective date: January 15, 2013 Policy owner: Chief Privacy & Security Officer Last Revised Date: July 2014 Next Review: 2018 Contact: Director, Information Technology Approved by: Strategic Management Committee</p>	Page 2 of 7

- the Government of Ontario’s Information Security & Privacy Classification Guide as a baseline for asset valuation. This standard has been widely adopted in the Ontario healthcare sector and sets an appropriate tone for asset valuation in a holistic manner.
- ii. Information in a ‘final’ or published state that is either in the custody of or produced and owned by CPAC must be classified into one of the following four categories:
- **Public** — information that is available to the public, employees, consultants and contractors working for the Partnership.
 - **Internal** — information that is available to employees and authorized non-employees (consultants and contractors) possessing a need to know for business-related purposes.
 - **Confidential** — information that is sensitive within CPAC and is intended for use only by specified groups of employees. A breach of such information could cause serious embarrassment and possibly undermine public trust in the organization.
 - **Restricted** — information that is extremely sensitive and is intended for use by named individuals or positions only. A breach of security would risk the health, safety, privacy or reputation of an individual, members of the public, subscribers, CPAC and its employees, consultants and contractors or client organizations.
- Refer to the table on the following pages for details associated with each information class.*
- iii. All CPAC employees, consultants and contractors who handle information in CPAC’s custody or under its control are responsible for understanding and implementing this policy.
- iv. All CPAC employees, consultants and contractors who apply privacy and security controls to CPAC’s IT Systems must ensure that those controls are appropriate and proportional to the sensitivity of the information under stewardship.
- v. All information classified as Internal, Confidential or Restricted must have privacy and security controls applied which are sufficient to ensure that the information is accessible only to those users who are authorised for access.

Information Classification Policy

Effective date: January 15, 2013
Policy owner: Chief Privacy & Security Officer
Last Revised Date: July 2014
Next Review: 2018
Contact: Director, Information Technology
Approved by: Strategic Management Committee

Classification	Description	Information Asset Examples	Risk Impact	Security Access Requirement
Public	Public information is available to the general public, partners and employees.	<ul style="list-style-type: none"> • Website content • Published reports • Marketing materials • Job postings • External Presentations 	<ul style="list-style-type: none"> • No impact • Minimal inconvenience if not available 	None
Internal	Internal information is available to employees and authorized non-employees (consultants and contractors) possessing a need to know for business-related purposes.	<ul style="list-style-type: none"> • Planning documents • Project status reports • Meeting Agendas and minutes • Documents containing work contact information • Strategic Planning documents • Operational documents • Policies and procedures • Policy advice 	<ul style="list-style-type: none"> • Disruption to business if not available • Low degree of risk if corrupted or modified 	Enhanced one-factor user Authentication to CPAC's network and Records Management System is required

Information Classification Policy


Effective date: January 15, 2013
Policy owner: Chief Privacy & Security Officer
Last Revised Date: July 2014
Next Review: 2018
Contact: Director, Information Technology
Approved by: Strategic Management Committee

Classification	Description	Information Asset Examples	Risk Impact	Security Access Requirement
Confidential	Confidential information is available only to a specific function, group or role.	<ul style="list-style-type: none"> • Personnel files • Banking information of non CPAC personnel • Contracts • Financial reports • Executive Committee of the Board - deliberations and supporting documents • Other Committees of the Board • Partner Information designated as sensitive; • 3rd party business information submitted in confidence • Compensation information • Legal Advice • Electronic Signature files • RFP and/or Funding Applications that are not awarded • Voice recordings of meetings 	<ul style="list-style-type: none"> • Loss of reputation or competitive advantage • Loss of confidence in the Partnership • Loss of personal or individual privacy • Loss of intellectual property • Loss of opportunity • Financial loss • High degree of risk if corrupted or modified • Compromise of board deliberations • Privacy breach • Destruction of partnerships and relationships 	Folder level access control to authorized users only
Restricted	Restricted information is available only to named	<ul style="list-style-type: none"> • Criminal records and/or investigations • Litigation records 	<ul style="list-style-type: none"> • Extreme or serious injury • Loss of public safety 	

Information Classification Policy

Effective date: January 15, 2013
Policy owner: Chief Privacy & Security Officer
Last Revised Date: July 2014
Next Review: 2018
Contact: Director, Information Technology
Approved by: Strategic Management Committee

Classification	Description	Information Asset Examples	Risk Impact	Security Access Requirement
	individuals or specified positions.	<ul style="list-style-type: none"> • Databases such as Cancer Registry, only named individuals have access • Personal Health Information as described in the Ontario Personal Health Information and Protection Act (PHIPA). 	<ul style="list-style-type: none"> • Significant financial loss • Significant legal implications • Significant damage 	Two-factor user authentication is required

 CANADIAN PARTNERSHIP AGAINST CANCER PARTENARIAT CANADIEN CONTRE LE CANCER	Information Classification Policy	
	Effective date: January 15, 2013 Policy owner: Chief Privacy & Security Officer Last Revised Date: July 2014 Next Review: 2018 Contact: Director, Information Technology Approved by: Strategic Management Committee	Page 6 of 7


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
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.
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.

 <p>CANADIAN PARTNERSHIP AGAINST CANCER</p> <p>PARTENARIAT CANADIEN CONTRE LE CANCER</p>	Information Classification Policy	
	<p>Effective date: January 15, 2013 Policy owner: Chief Privacy & Security Officer Last Revised Date: July 2014 Next Review: 2018 Contact: Director, Information Technology Approved by: Strategic Management Committee</p>	Page 7 of 7

<p>Enhanced one-factor and two-factor user authentication</p>	<p>Access to some of CPAC’s information or information technology may require enhanced one-factor or two-factor user authentication. Enhanced one-factor authentication requires two pieces of information about a user that is known to an authorized person before access is authorized. 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). Authentication factors may include:</p> <ul style="list-style-type: none"> • A valid username and password, issued by CPAC to an individual, for the purpose of accessing designated CPAC information or information technology. • Physical security clearance to CPAC facilities, such as valid elevator and/or floor/area access passes. • A contractual relationship between CPAC and a third-party organization, wherein the organization agrees to ensure that the user, being an employee or agent of the organization, will comply with applicable CPAC privacy and security policies. • A security token, issued to an individual, for the purpose of accessing designated CPAC information or information technology.
--	--

1.7 Related Documents

- [Information Management Policy](#)
- [Records Management Policy](#)
- [Information and Information Technology \(I&IT\) Security Policy](#)
- [Protection of Personal Information Policy](#)
- [Acceptable Use Policy](#)

End of document