CANADIAN PARTNERSHIP AGAINST CANCER

PARTENARIAT CANADIEN CONTRE LE CANCER

Cybersecurity Policy

As of May 2020

POLICY PURPOSE

1. The CPAC Cybersecurity Policy describes how we protect the security of our data and technology infrastructure.

POLICY RATIONALE

1. Cybersecurity means that CPAC's information is protected in accordance with its value, sensitivity, and regulatory obligations.

2. As CPAC expands its online services, it creates, manages, and shares increasingly more information online with data protection requirements.

3. CPAC relies heavily on technology to collect, store, manage, and *protect* our business information and sensitive data.

4. This all makes CPAC increasingly vulnerable to cybersecurity incidents. Human errors, email phishing attacks, malware, accidents and breaches have the ability to jeopardize CPAC's online presence, reputation, and identity.

PRINCIPLES

1. This policy is based on the following core principles:

    a. Information will be protected against any unauthorized access;
    b. Confidentiality of information will be assured;
    c. Integrity of information will be maintained;
    d. Availability of information for business processes will be maintained;
    e. Legislative and regulatory requirements will be met;
    f. Information security training will be provided to all employees;
    g. All actual and suspected information security breaches will be reported.

2. A Cybersecurity Manual, maintained by the Director, Information Technology supports the implementation of this policy with detailed standards and guidelines.

3. All employees must report actual or suspected cybersecurity incidents, including information breaches, to their immediate supervisor as applicable as soon as possible for escalation to the Director, Information Technology.

4. All staff, contractors, and third parties must comply with the Cybersecurity Policy.

DEFINITIONS

- Cloud Services – information technology services offered where the location of the computing infrastructure is not located at CPAC facilities.

- Cloud Service Provider – a company that offers cloud computing services, typically in the form of Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS"), and Software-as-a-Service ("SaaS")
  - *See also: Third-Party Service Provider*

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

- Cybersecurity Framework - an established reference model and standard to establish, measure, and define a cybersecurity program. It includes:
  - Risk Identification considers the criticality and sensitivity of CPAC information, systems, cybersecurity threats and vulnerabilities.
  - Information Protection considers technical safeguards (such as encryption), vulnerability management (such as patching and hardening), Operational practices in IS operations and application development, and repeatable processes; information governance.
  - Incident Detection considers the use of monitoring, logging, and threat analytics.
  - Incident Response considers triage, escalation, containment and closure coordinated organization-wide; in conjunction with teams incident response.
  - Recovery results in continuous risk management and maturity improvements.

- 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.

- Cybersecurity Manual - describes cybersecurity standards and processes on shared IT systems, networks, cloud services, and provides a reference baseline standard organization-wide.

- Cybersecurity Program – a program focused on the protection of IT systems, computer security, CPAC's ability to prevent, detect, and respond to Cybersecurity

attacks. The Cybersecurity Program is based on the NIST Cybersecurity Framework.

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

- Information Security Incident – any incident or series of events that may have an adverse effect on CPAC's Information Technology and/or network that poses a threat to asset or network security in respect of availability, integrity and confidentiality.

- Information Technology (IT) – any arrangement of networks, technical infrastructure, applications and end user technology that is connected, owned and/or operated by an organization.

- Incident Response Plan – a set of written processes and instructions for coordinated implementation of cybersecurity incident detection, response and recovery as part of the Cybersecurity Program.

- IT Risk Register – a prioritized listing of all **major** cybersecurity risks.

- Network Device – A device to which network cables are attached. These devices may filter, connect, control, or address network traffic. Bridges, Hubs, Switches and Routers are examples of Network Devices

- Payment Card Industry (PCI) - the segment of the financial industry that governs the use of all electronic forms of payment.

- Privacy Incident – the loss of, unauthorized access to, or disclosure of personal information.

- Removeable Storage Media - USB flash drives, external/portable hard drives, memory cards, DVDs, CDs, etc.

- Third-Party Service Provider – any consultant, agent, advisor or independent contractor who renders services to CPAC. This includes Cloud-Service Providers.

RESPONSIBILITIES

2.01 CPAC Executive Committee

a) Receive, review and adopt this policy and any recommended amendments thereto.
b) Ensure organizational adherence to the Cybersecurity Policy.
c) Without limiting the general statement in (b), delegate the powers, duties and functions of the CPAC Executives as necessary to give effect to this Policy.

2.02 Chief Privacy and Security Officer ("CPSO")

a) Establish and maintain the Cybersecurity Program (including process, policies, tools, training and standards) to ensure CPAC's electronic information and Systems and Services are adequately protected in accordance with the Cybersecurity Policy and associated standards.
b) Review and approve third-party services, including cloud providers.
c) Assist the executive team with reporting and manage the reporting of serious incidents to external authorities.
d) Without limiting the general statement in (b), delegate the powers, duties and functions of the CPSO as necessary to give effect to this Policy.

2.03 Director, Information Technology

a) Develop and maintain the Cybersecurity Manual.
b) Review and revise, as needed, the Cybersecurity Manual on a biennial basis.
c) Conduct cybersecurity assessments as needed.
d) Monitor and manage cybersecurity operations of CPAC Systems and Services, shared information technology systems and connections, cloud services, and third-party information providers.
e) Develop, implement, and evaluate CPAC's cybersecurity awareness training program.
f) Evaluate, assist, and report on cybersecurity activities.
g) Provide expert security advice and independent security review and assessment to project leads, management and stakeholders.
h) Maintain the CPAC IT Risk Register and Action Plan.
i) Manage cybersecurity incident response in coordination with team heads.
j) Implement, monitor, review, and ensure compliance with applicable cybersecurity standards.
k) Report to the CPSO and CPAC Executive regarding key risks, compliance, and significant activities related to cybersecurity. Serious incidents must be reported immediately to the CPSO and Executive Committee.

l) Report on key risk indicators, team compliance and activities in relation to cybersecurity.

2.04 Managers and Directors

a) Support the implementation of, and compliance with, the Cybersecurity Program and related standards.
b) Ensure that all Authorized Users within their team have had the opportunity to read this policy and obtain clarification on this policy.
c) Provide support as needed to the Director, Information Technology in their assessment of risk mitigation strategies and status of compliance with respect to the cybersecurity of the technology operated by the teams not under the direct control of the IT Team.
d) Report all suspected and real cybersecurity vulnerabilities and incidents to the IT Service Manager and/or the IT Managed Service Provider's Service Desk, with escalation to the Director, Information Technology.
e) Implement, monitor, review, and ensure compliance with the standards and procedures identified in Cybersecurity Manual that are in within their area of responsibility.

2.05 Information Technology Employees ("IT Team")

a) Operate the Cybersecurity Program with responsibilities in Cybersecurity Incident handling, and Cybersecurity operations.
b) Support the Director, Information Technology in maintaining the CPAC information security risk register and IS risk management process.
c) Maintain the Cybersecurity Manual, and support standards and processes.
d) Implement, monitor, review, and ensure compliance with the policies, standards and procedures identified in the Cybersecurity Manual.
e) Work with CPAC's IT Managed Service Provider to respond to cybersecurity incidents.
f) Record and Report on cybersecurity incidents and vulnerabilities as discovered.

2.06 IT Managed Service Provider

a) Implement information technology system process and technology changes in accordance with CPAC's Cybersecurity policies and standards, including incident response. `
b) Ensure latest security application and operating system security patches are applied for all managed devices.
c) Detect, respond, recover, and enact protective against cybersecurity incidents at the direction of the IT Service Manager.
d) Communicate any vulnerabilities discovered to CPAC's IT Service Manager.

e) Provide CPAC's IT Team with network activity logs or logs containing anomalous activity upon request/discovery.

2.07 Computer Security Incident Response Team ("CSIRT")

a) As required by the CPSO or the Director, Information Technology, contain, investigate, remediate and report on information security incidents.
b) Respond to Privacy Incidents when required and as determined by the CPSO.

2.08 All Employees, Contractors and Third Parties

a) Report actual or suspected cybersecurity breaches or potential Cybersecurity Incidents to their immediate supervisor as soon as possible for escalation to the Director, Information Technology.
b) Comply with all applicable provisions of the Cybersecurity Manual.
c) Responsible for the appropriate use of CPAC systems in accordance with the CPAC Acceptable Use Standard.