Information and Information Technology Security Policy

1.1 Overview

In today's high-tech and interconnected world, the Partnership needs security front and centre in order to protect its information and information technology assets from threats that exist from internal and external sources. Pursuant to this goal, this Policy provides management direction to the Partnership on what needs to be done to secure corporate information and technology assets. Further, the Information and Information Technology Security Policy is a cornerstone policy that supports the Partnership's greater vision of risk management as described in the Partnership's Enterprise Risk Management (ERM) Policy which establishes the criteria within which risk is managed at the Partnership. Details associated with how this Policy on Information and Information Technology Security should be implemented can be found in other components of the Partnership's Privacy and Security Framework. The Partnership may impose additional direction at its discretion.

1.2 Purpose

The purpose for this policy is to define rules for configuring and managing security in a way that protects the Partnership's information and information technology assets.. The rules are based on the following international standards:

i. ISO/IEC 27001, the 'Standard for an Information Security Management System'.
ii. ISO/IEC 27002, the 'Code of Practice for Information Security Management'.
iii. ISO/IEC 27005, the 'Standard for Information Security Risk Management'.

Through this policy, the Partnership can minimize its risks and show due diligence to its partners, stakeholders and the general public. All Partnership 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 Partnership employees, consultants and contractors who access the Partnership's information assets using the Partnership's information technology assets.

1.4 Policy Statements

1.4.1 Governance

i. The Partnership's Chief Privacy and Security Officer is responsible for issuing and monitoring compliance with this Policy.

ii. The Partnership's Chief Privacy and Security Officer must ensure that this Policy is reviewed periodically and updated when required.

1.4.2 Organization Responsibilities

i. Management must set direction and provide support for this Policy.

ii. Management must confirm organizational compliance with this Policy at least once every two years.

1.4.3 Asset Management

i. An inventory of all important assets (tangible or intangible) associated with information and information technology must be documented and maintained.

ii. Owners must be designated for all assets associated with the processing and storage of information.

iii. Rules for the acceptable uses and disposal of the Partnership's assets must be identified, documented, and implemented.

1.4.4 Information Classification

i. The Partnership must define classes of information based on sensitivity levels.

ii. Security and privacy assessments conducted by or on behalf of the Partnership must leverage the Partnership's Classification Schedule.

iii. Information must be identified, labeled when appropriate, and handled in accordance with the Partnership's Classification Schedule.

1.4.5 Human Resources Security

i. Employees, consultants and contractors must be screened prior to entering a working relationship with the Partnership, and the level of scrutiny must be appropriate for the trust level required to fulfill the duties associated with the working relationship. As an example, individuals who require access to **Confidential** or **Restricted** information as part of their role should undergo a Canadian Police Information Center (CPIC) background check.

ii. Employees, consultants and contractors who require access to **Confidential** or **Restricted** information as part of their role must sign the Partnership's Non-Disclosure Agreement (NDA).
iii. Employees, consultants and contractors must receive appropriate information and information technology security awareness training, and be informed of changes to this Policy.
iv. Security responsibilities regarding termination of employment (or other type of relationship) must be documented.
v. Employees, consultants and contractors must return the Partnership's assets upon termination of their relationship with the Partnership, or upon change of employment or other type of relationship if appropriate.
vi. The access rights of employees, consultants and contractors to information and information technology must be removed immediately upon termination of employment or other type of relationship, and reviewed upon change of employment or other type of relationship.

1.4.6 Physical and Environmental Security

i. The Partnership's information processing facilities (e.g. data centre and LAN closets) must be protected by a physical security perimeter.
ii. Physical security requirements must be designed, documented, and applied for all areas in and around an information processing facility.
iii. The Partnership work areas must be protected with appropriate entry controls to ensure that only authorized personnel are allowed access. As an example, visitors and service personnel may not enter the Partnership work areas unless escorted by a Partnership employee.

1.4.7 Equipment Security

i. Equipment must be protected, commensurate with its availability requirements, from power supply interruption and other disruptions caused by failures in supporting utilities.
ii. Power and telecommunications cabling must be protected from interception and damage.
iii. Equipment must be correctly maintained to enable continued availability and integrity.
iv. Equipment must be protected using documented security controls when off-site from the Partnership's premises. An example of a control could be that files or laptops are not to be left in unlocked cars or on seats where they are visible by passers-by.
v. Information, records, and software must be protected against unauthorized disclosure during and subsequent to the reassignment or destruction of hardware and media.

vi. Equipment, information, or software belonging to or under the control of CPAC must not be removed from the Partnership's premises or leased locations without prior authorization.

vii. Onsite laptop computers must be secured at all times (e.g. locked when not in use to a permanent fixture, locked in a filing cabinet if a locked office is not available).

1.4.8 IT Infrastructure Security

i. IT infrastructure (e.g. servers and the corporate network) constitutes the backbone of services that the Partnership delivers in fulfilling its mandate. The effective implementation of security across all IT infrastructure components will minimize the risk of unauthorized access and use of the Partnership's information and information technology. Accordingly, the Partnership must document and implement best practices to secure its IT Infrastructure.

1.4.9 User Name, Password and Administrative Controls

i. User names, passwords and other similar administrative controls constitute a critical underpinning of computer security. They are the front line of protection for user accounts. Poorly constructed user names and passwords may weaken the security of the Partnership's information technology. Accordingly the Partnership must document and implement best practices related to password strength and complexity, acceptable encryption, and other similar administrative controls.

1.4.10 Mobile Devices

i. Since the Partnership employees will connect to the corporate network using a mobile device, private and confidential information must be protected from deliberate or inadvertent exposure which could result in loss of information, damage to critical applications and damage to the Partnership's reputation. Accordingly the Partnership must document and implement best practices related to usage of corporate and personal mobile devices to access the corporate network and corporate systems.

1.4.11 Storage Media Destruction

i. The Partnership creates, collects, stores and processes personal information, and sensitive business information which constitutes the Partnership's intellectual property. Discarding redundant computers, laptops and electronic media without securely destroying the sensitive data within unduly exposes the Partnership to breaches of privacy and/or litigation. Accordingly the Partnership must document and implement effective media

destruction controls in a way that renders the information contained within to be unrecoverable.

1.4.12 Access to the Partnership's Information and Information Technology

I. Access to the Partnership's information or information technology must be controlled in a manner commensurate with the criticality and sensitivity of the information or information technology being accessed and must leverage a secure logon process.
   a) All access to the Partnership's information or information technology must follow a defined and tracked Authorization process, with an appropriate system, business or information owner formally authorizing access.
   b) The assignment of system privileges or authorization of access must be restricted and controlled following least privilege and separation of duty principles.
   c) Users must only be provided access to the information systems and technology they have been specifically authorized to use.
   d) During authorization, restrictions on connection and times must be established and implemented to provide additional security for high sensitivity applications.

II. Third party access to the Partnership's information or information technology must leverage authorization controls commensurate with the criticality and sensitivity of the information or information technology being accessed.
   a) Third party organizations must agree in writing or in contract to ensure that any user, being an employee or agent of the organization, will comply with applicable Partnership privacy and security policies, prior to being authorized for access.

III. All access to the Partnership's information or information technology must leverage appropriate authentication techniques and mechanisms commensurate with the criticality and sensitivity of the information or information technology being accessed. Options for authentication may include;
   a) Username and password
   b) Enhanced one-factor authentication which requires the submission of two pieces of information about a user for authentication to occur.
   c) Two-factor authentication which requires two independent factors about a user about a user for authentication to occur. (e.g. something that is held by an authorized person, and something that is known to an authorized person).

d) Authentication must, at a minimum include a valid username and password, issued by the Partnership to an individual, for the purpose of accessing Partnership information or information technology.
e) Access to the Partnership's information or information technology must consider the use of enhanced authentication including the use of security tokens.
f) Strong or enhanced authentication must be employed in controlling access to **Confidential** information.
g) Two factor authentication must be employed in managing access to **Restricted** Information
h) All remote access to Partnership information from a non-corporate device must leverage two-factor authentication

IV. Third party access to Partnership information or information technology must leverage authentication controls commensurate with the criticality and sensitivity of the information or information technology being accessed.
   a) Third party access to Partnership information or information technology must consider the use of enhanced or two-factor authentication including the use of security tokens when accessing Partnership information or information technology.
   b) The Partnership must document and implement policies and best practices related to access and release of personal information to third parties.

1.4.13 Protection of Partnership Technology and Information

i. All personnel and employees must possess a valid office Security pass or clearance to Partnership facilities, such as valid elevator and/or floor/area access passes.

ii. Users must ensure unattended equipment has appropriate protection.

iii. Users must ensure the safety of sensitive information, both digital and paper, and protect it from unauthorized access, loss, or damage. Users must ensure that passwords, secure tokens, digital certificates, and any other identifiers used by the user to directly or indirectly gain access to the products, services, or technology infrastructure are safeguarded.

iv. All removable computer media must be managed with controls appropriate to the highest level of sensitivity of the data contained on the media. All removable computer media must be scanned prior to attaching to the corporate network.

v. Third party information exchange policies, procedures, and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services.

vi. Information and software exchange agreements between the Partnership and other organizations or third parties must be documented, and contain security and privacy requirements and defined roles and responsibilities for security and privacy.

vii. Information in web services/transactional information systems must be protected from fraudulent activity, repudiation, unauthorized disclosure, and modification.

viii. Information systems utilizing web services/on-line transactions must have security controls commensurate with the value and classification of the information.

1.4.14 Network and Network Equipment Security

i. Physical and logical access to diagnostic ports must be securely controlled.

ii. Groups of information services, users, and information systems must be segregated on networks to establish a zoned access model.

iii. Use of system utility programs that manage and control systems and the Partnership's network must be restricted to authorized users only and tightly controlled.

iv. Appropriate network security controls must be implemented to achieve and maintain security within the Partnership's network in line with defined risk tolerances.

v. Inactive sessions must be locked after a defined period of inactivity.

vi. Prevention, and detection controls must be utilized to protect information technology against malicious code.

vii. Media being physically transported must be appropriately protected either with physical secure locks or device encryption.

1.4.15 Operations

i. Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained.

ii. Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems.

iii. Security features and expectations, Vendor and The Partnership roles and responsibilities, service levels, and management requirements of all network services must be documented and included in any network service agreement.

iv. The use of information technology resources must be monitored, optimized, and projections made of future capacity requirements.

1.4.16 Monitoring and Oversight

i. Security requirements must be identified and addressed prior to granting external parties access to information or information technology. The Partnership must regularly monitor and review services, reports, and records provided by external parties and carry out regular audits.

ii. Audit logs must record user activities, exceptions, and information security events. The logs must be regularly reviewed as part of standard operating procedures, and will assist in access control monitoring and future investigations.

iii. Information system logging facilities and log information must be protected against tampering and unauthorized access.

iv. Key activities of privileged users should be subject to detailed periodic reviews.

v. Computer clocks shall be synchronized to a central and trusted time source for accurate reporting.

1.4.17 Change Management

i. Change management processes for information system services delivered by external parties must take into account the criticality of the information systems, processes involved and assessment of risks.

ii. Changes to information systems and information processing facilities must be controlled.

iii. Establishment of changes to existing information systems or information processing components requires an assessment of security risks that are to be used to inform approval.

iv. Development and staging environments for information systems must be separated from production (operational) environments.

v. All changes to technology and systems must be approved following a review from a Change Advisory Board (CAB)

1.4.18 Risk Assessment

i. Establishment of new information systems and infrastructure requires an assessment of security risks that are to be used to inform the Partnership's Certification Standard.

1.4.19 Training and Awareness

i. The Partnership must develop and manage an IM and IT Security awareness and training program for all employees.

1.4.20 Third Party Systems

i. The Partnership must authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

ii. The Partnership must authorize the use of all third party, non-Partnership owned technologies and cloud based services before they are used by employees.

iii. The Partnership must control the uploading, or transfer, of the Partnership's information to public. The Partnership must prevent unauthorised, or unapproved services from being used (e.g. Dropbox, SkyDrive, and Google Drive)

1.4.21 Electronic Storage of Confidential and Restricted Information

i. All **Confidential or Restricted** Information that is retained in electronic form must be stored on Partnership servers, such as the shared network drives or on physically secure stand-alone systems. This ensures that all Confidential or Restricted information leverages Partnership IT Systems that are backed-up regularly; have password protections enabled, and they are physically more secure than desktop and laptop computers.

ii. **Confidential or Restricted** Information must not be stored on laptops or USB drives unless encrypted, in accordance with the Partnership's Acceptable Encryption Standard and. These portable devices must be also stored in a secure area.

iii. **Confidential** or **Restricted** information must not be stored on mobile devices or other portable media as in accordance with the Mobile Device Policy.

iv. **Confidential** or **Restricted** information must not be stored or published/uploaded to any online services or collaboration tools unless approved by the Partnership's Director of IT.

1.4.22 Wireless Networks

i. Unmanaged, non CPC owned and operated wireless networks are prohibited to be used by the Partnership's information technology devices unless explicitly approved by the Director, IT. For further information, please refer to the Remote Access Standard.

1.4.23 Paper Printouts (Printer or Fax)

i. Printouts may contain **Confidential** or **Restricted** information. Individuals must retrieve printouts promptly, so as not to leave such printouts unattended at a printer or on an office desk.
ii. Printers or fax machines located in unattended common areas should not be used for **Confidential** or **Restricted** information unless printouts are password protected.
iii. Printouts containing Confidential or Restricted information must be safely disposed of using designated shredder boxes.

1.4.24 Social Networking and Related Tools

i. Users of the Partnership's information technology who participate in Social Networking are subject to the guidelines and terms defined in the Partnership's Social Media and Acceptable Use Policies.
ii. The use of social media and productivity or team collaborative tools not owned or managed by the Partnership must be formal authorized and approved prior to their use.

1.4.25 Remote Access to Partnership Systems

i. Access to the Partnership's IT Systems from off-premises is granted in accordance with the Remote Access Standard. Employees who access the Partnership's IT Systems from off-premises are required to be familiar with this Standard, and to actively ensure that such access meets all of the requirements.

1.4.26 Audit, and Vulnerability Management

i. Users of the Partnership's information technology who are responsible for auditing and vulnerability management are subject to the terms defined in the Partnership's Audit and Vulnerability Management Standard, and the Patch Management Standard.

1.4.27 Information Security Incident Management

i. Information security events must be reported through appropriate channels as quickly as possible as per the Information Security Incident Procedure.
ii. Individuals using the Partnership's information technology must note and report any observed or suspected security weaknesses in the technology.
iii. Incident management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

iv. The types, volumes, and costs associated with information security incidents must be quantified and reported on, and monitored as needed.

v. Rules must be defined for collection of evidence in the context of investigating security incidents.

vi. Investigations into information security incidents must ensure evidence is collected, retained, and presented in conformance with the Partnership's standards on incident response and rules for collection of evidence.

1.4.28 Business Continuity Management

i. A risk assessment must be conducted to identify information and information technology security events that may interrupt business processes. This risk assessment may be conducted as part of the Partnership's Certification and Accreditation Standards.

ii. Plans must be developed to maintain or restore business operations following interruption or failure of essential services.

iii. A business continuity plan must address information and information technology security requirements.

iv. Business continuity and/or IT Disaster Recovery plans must be regularly tested and updated.

v. Information and information technology systems must be backed up and the recovery process documented, and tested regularly.

vi. Systems design and configuration documentation must be protected from unauthorized access.

1.4.29 System Certification

i. The purpose of system certification is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The purpose of certification is to signify that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service, based on the certification evidence. The graduated performance of certification depends upon the quantity and quality of certification evidence required by the certification authority. Such evidence can include the results of any applicable Threat and Risk Assessment, a Business Impact Assessment, a Privacy Impact Assessment, a Vulnerability Assessment, security tests and product evaluation, self-assessments, audits and security reviews and related legal or policy assessments that demonstrate conformance to relevant legislation or policy. Accordingly:

a) The Partnership must maintain a system certification standard, and certify all sensitive IT systems and services prior to operation or in a reasonable time after implementation.
b) The Partnership must periodically review the certification of systems or services if the systems or services have changed significantly or if warranted due to changes in the risk environment.

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 Partnership 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
Confidential Information	Information that is sensitive within the Partnership 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.
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 Partnership 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 the Partnership to be an information and information technology asset.

Term	Definition
Privacy and Security Framework	A framework of policies, standards, processes, procedures, templates and tools designed to be used independently and collectively to protect the privacy and security of the Partnership's information and information technology assets.
Restricted Information	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, the Partnership and its employees, consultants, vendors, or client organizations.
User	Any person who accesses and uses CPAC resources.

1.7 Related Documents

- Information Classification Policy
- Acceptable Use Policy
- Protection of Personal Information Policy
- Mobile Devices Policy
- Bring Your Own Device (BYOD) Policy
- Information Management Policy
- Records Management Policy and Procedures
- Media Destruction Standard
- Acceptable Encryption Standard
- Audit and Vulnerability Management Standard
- Remote Access Standard
- Password Standard
- Electronic Mail Standard
- Patch Management Standard
- System Certification Standard
- IT Infrastructure Security Standard
- Information Security Incident Procedure
- Social Media Policy
- Enterprise Risk Management Policy

End of Document