Information Management Policy

1.1 Overview

The management of information assets is a core component of CPAC operations. Information assets form the intellectual capital on which CPAC relies for service delivery. Best practises, policies and standards that result in efficient, accountable and cost-effective use of information resources. Information management ensures that critical characteristics such as authenticity, reliability, integrity and usability of information are preserved and protected throughout the information lifecycle.

CPAC must appropriately provide access to, manage, preserve and dispose of its information assets in accordance with relevant legislation, policies and standards, in order to:

i. Ensure accountability.
ii. Provide evidence of its activities and organizational structure.
iii. Document its responsibilities, privileges and entitlements.
iv. Preserve information assets of enduring value.

This Policy provides management direction to the organization on what needs to be done in terms of managing information; it does not specify how the Policy should be implemented. Details associated with how the Policy should be implemented can be found in CPAC's Cybersecurity Policy Standards Manual. CPAC may impose additional direction at its discretion.

1.2 Purpose

The purpose for this policy is to define rules for managing information in a way that protects the privacy and security of CPAC's information assets. The rules:

i. Assign responsibility and accountability for the management of information in CPAC's custody or under its control. All CPAC employees will receive privacy and security awareness training to support their understanding and adherence to this policy.
ii. Facilitate compliance with relevant legislation, policies and standards.
iii. Promote the creation and retention of a full and accurate record, documenting decisions and actions for official records.
iv. Require that relevant information is provided in a timely, useable, cost-effective, and accurate manner.

v. Enable the preservation of CPAC information in a manner that retains the information's authenticity, reliability, accessibility and integrity for as long as required.
vi. Support transparent and effective access to information assets within legally established privacy and confidentiality restrictions.

1.3 Scope

This policy applies to all CPAC employees, consultants and contractors who manage CPAC's information assets, and/or develop operational procedures, standards and policies to govern the management of CPAC's information assets.

1.4 Policy Statements

1.4.1 Governance of Information

i. CPAC must manage all information created and received during the conducting of its business activities.
ii. CPAC must establish and maintain an information management program to manage the design, integrity, availability, and efficient use of information management systems.
iii. Information assets must be identified, classified, inventoried, documented and maintained throughout their lifecycle.
iv. CPAC official records must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.

1.4.2 Classification and Retention of CPAC Information

i. CPAC must develop, implement and maintain a Records Management System, with detailed, ongoing information retention and disposal schedules to manage all documents and information in an electronic format.
ii. CPAC must develop, maintain and promote an information classification schema for all CPAC information assets.
iii. CPAC information must remain authentic, reliable and accessible after any conversion or migration from one media, format, or system to another.

1.4.3 Storage and Disposal of CPAC Information

i. CPAC information must be disposed of securely in accordance with approved information retention and disposal schedules and asset management processes as defined in CPAC's Cybersecurity Manual.
ii. CPAC information scheduled for archival retention must be maintained in a manner that preserves their integrity and authenticity up to and throughout transfer to CPAC archives.
iii. CPAC information scheduled for destruction must be destroyed in a method appropriate to the information media upon which it is stored and that maintains the security of the information and the privacy of individuals. Official business records and communications, such as documents of historical significance, email or instant messages may be exempt from destruction in accordance with this policy.

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 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; and/or Prosecution under law.

1.6 Definitions

Term	Definition
Information 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.
Official Records	Official Records are those records which provide the most complete and conclusive information on a specific action or event. The Official Record may be a blend of multiple

	media. Electronic records may constitute the Official Record. Responsibility for retaining the official record is assigned in the Record Classification Structure. Official Records: • Are required to support operations. • Document and provide evidence of transactions. • Provide evidence of compliance with accountability or other requirements. • Will have some future financial, legal, research or archival value.

1.7 Related Documents - Records Management folder link

- Privacy Statement
- Cybersecurity Policy
- Cybersecurity Policy Standards Manual
- Records Management Policy

End of Document