Media Destruction Standard

1.1 Overview

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

To ensure that personal and business information in CPAC's custody or under its control remains secured appropriately, effective media destruction 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 media destruction in the context of personal and business-related information in CPAC's custody or under its control.

Media destruction ways and means will:

i. Prevent violation of software license agreements.
ii. Prevent unauthorized release or disclosure of personal information.
iii. Prevent unauthorized release or disclosure of trade secrets, copyrights, and other intellectual property.

1.3 Scope

This standard is mandatory and applies to all CPAC employees, consultants and contractors who are responsible for the destruction, transfer or re-use of data storage media.

1.4 Standards

i. CPAC employees, consultants and contractors are not permitted to destroy electronic storage media containing information. If such media requires destruction, users must notify the CPAC IT Service Desk to facilitate such destruction.

ii. Data stored on any CPAC electronic media (e.g. laptops, desktops, CDs, backup tapes) must be permanently destroyed by the IT Department whenever the storage media is declared surplus, declared obsolete, returned at the end of a leasing period, replaced due to a failure of the media, replaced due to a failure of the media, replaced due to an upgrade of the media, or when an explicit request for destruction is received by the IT Department from a data owner.

iii. All data on CPAC electronic storage media must be securely erased using CPAC's approved certified data erasure product.
   - A minimum of five (5) passes must be conducted on the disk to be erased, so as to ensure that the data has been rendered permanently inaccessible.
   - A report must be generated for all data destruction activities, and the report must be signed by CPAC's IT Department and notification provided to the CPSO. The report must be attached to the Data Storage Media Destruction Request Form and stored in Records Management for audit purposes.

iv. Any partner/vendor that holds personal information or business-related information on behalf of CPAC must ensure that media destruction has taken place in compliance with this Standard, and issue a formal confirmation of destruction to CPAC's IT Department.

v. Licensed software residing on electronic storage media that is destroyed is deemed to have been destroyed through this procedure.

1.5 Enforcement

Failure to comply with this standard may result in actions by CPAC 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; and/or Prosecution under law.

1.6 Definitions

Term	Definition
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.
Data Owner	An Individual or entity that can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

1.7 Related Documents

- Information Management Policy
- Information and Information Technology (I&IT) Security Policy
- IT Infrastructure Standard
- Records Management Policy
- Records Management Procedures

End of Document