Office of the Chief Information Officer

INFORMATION TECHNOLOGY SECURITY - ASSET DISPOSAL

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

March 1, 2012

Keywords: Information Storage Assets, Storage Media, Asset Investment Recovery, IT Asset Disposal Management Process, Risk Level, Information Security Classification, Records

Description of Standard

The IT Asset Disposal Standard defines the decommissioning method to dispose of IT storage assets securely. This Standard ensures implementation of security controls on storage media to prevent unauthorized release of information through sale or disposal. Safeguards confidential information is processed securely at the end of its lifecycle in accordance with established policies.

The life cycle of IT assets including information stored on them, starts with creation to removal/deletion or disposal of the information and the IT asset. When information is collected, it is stored in a media capable of storing electronic information. Storage media is used to store information, transport information between computers or backup and safeguard information for extended periods of time. Storage media may consist of hard drives, memory cards, tapes, portable storage devices (e.g.: USB keys, CD/DVD, floppy/hard disks and other electronic storage media (e.g.: SmartPhones, Multi-Function Devices, Laptop /Tablets /Servers, and Network Devices – Routers/Switches/Appliances). For securing data, the life cycle needs to be managed. The secured information at the end of the life cycle is critical to eliminate failure points and minimizing the risk of a breach of confidential information.

The Ministry Information Security Officer (MISO) is responsible for supporting business owners and areas in implementing the disposal process for IT assets by:

- Confirming IT asset(s) ownership and appropriate approvals for disposal.
- Responsible for adhering to records management policy, ARCS/ORCS, and security classification requirements.
- Confirming information contained on the device is not currently subject to any known litigation discoveries or requests for information under the Freedom of Information and Protection of Privacy Act.
- Ensuring implementation of controls to identify and secure information technology assets and prevent unauthorized release of information through sale or disposal.
- Responsible for having the IT Asset Disposal Submission Form completed.
- Securely storing the IT assets until pick up.

IT asset(s) with storage media being considered for resale must observe the following storage erasing (sanitization) process. At a minimum, the following must be provided:

1) Documentation of the relevant serial number(s), asset tag(s), Ministry and/or location, associated software license(s) and other pertinent details about the device, such as primary owner/user.

2) The information on the device is rendered inaccessible either by:

A commercially proven/certified data erasure solution which meets the international erasure standard: US Department of Defense Sanitizing (DOD 5220.22-M, DOD 5220.22-M ECE) and can generate a Certificate of Destruction or Erase Audit Report, or;

a) Encryption of the storage device and subsequent data erasure with a single pass overwrite solution, or;

b) Deletion of the encryption key for devices that were encrypted using government standard.

3) Documented attestation that all steps have been satisfactorily completed, including a detailed report at the end of the erasure process showing erasure was successful.

Any IT Assets which cannot meet the minimum storage erasure requirements as stated must be sent securely for destruction through Asset Inventory Recovery (AIR). Processes for securing assets for resale and disposal are defined in the Disposal Handbook.

Where to Apply This Standard

The Standard applies to Ministries, the Broader Public Service (BPS) and Contractors that have been assigned a government device and are required to dispose of that IT device or has government data on their personal device. The Standard is aligned with Asset Investment Recovery's (AIR) process and procedures in conjunction with Chapter 6 of the Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia.

Authority and Exemptions

This standard has been issued by the OCIO in order to insure the protection of government information through the safe and secure disposal of government IT information storage assets in a manner that is consistent with policy, applicable legislation, and contract law. If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the OCIO.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the protection of government information assets, ministries and other government agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance through random audits and forensic erasure verification inspections are conducted throughout the decommissioning process and discrepancies in the results reported to the Government Chief Information Officer.

Terms and Definitions

Terms and definitions are defined within the standard.

References

The authority to dispose of tangible property has been delegated to Logistics and Business Services (LBS) in Shared Services BC (SSBC). Within LBS, explicit authority has been delegated to the Asset Investment Recovery (AIR) Branch for tangible asset disposals.

The Core Policy and Procedures Manual (CPPM) contains government-wide policies for managing information, communications, materiel, transportations, contracts and expenses. AIR is responsible for the disposal of surplus tangible assets of the Province of BC. The administrative authority comes from section 6.3.4 of government's Core Policy and Procedures Manual and the legal authority comes from section 2 (1) (f) of the Procurement Services Act.
Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia

Chapter 12 of CPPM specifically outlines the policies, authorities, responsibilities and guidelines for managing information and information technology within BC government.
Core Policy and Procedures Manual

Chapter **8** Asset Management and Information Security Policy.
Chapter 12 Destruction of Records and the Recorded Information Management Manual.
Chapter **15** Security.

> The Information Security Policy (ISP) provides a structured approach to identifying the broad spectrum of information security activities in the life -cycle of information systems. The Information Security Policy provides the framework for government organizations to establish local policies and procedures necessary for the protection of government information and technology assets.

Information Security Policy

Information Security Policy Summaries offer guidance on how the ISP applies to a subject areas: Policy Summary No. 2: Disposal of Information Storage Assets

Additional Information

Information Incident Management Process
Information Security Classification Standard

Further information on IT asset disposition is located on the IT Asset Disposition SharePoint site.

Contact

Information Security Branch
email: CITZCIOSecurity@gov.bc.ca