Mobile Device Disposal Interpretation and Guidance Document

This document is intended to provide guidance to Ministries and the Asset Investment Recovery Branch (AIR) in the interpretation of the “INFORMATION TECHNOLOGY (IT) SECURITY – ASSET DISPOSAL” Standard for Smart phones & Tablets.

Contents

OCIO location of standard:
http://www2.gov.bc.ca/gov/DownloadAsset?assetId=8CB29D9944C84E129C1258C18AD843A3&filename=it_asset_disposal_standard.pdf last updated March 1, 2012

Standards page:

http://www2.gov.bc.ca/gov/topic.page?id=2A477231EF934E22B0FBC8C43A98B9D9

OCIO Statement:

Abbreviated summary of the IT Asset Disposal Standard:
“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) 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;

b) Encryption of the storage device and subsequent data erasure with either:
- a single pass overwrite solution, or;
- 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.

Mobile Device Disposal Interpretation and Guidance Document

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, warranty and disposal are defined in the Disposal Handbook."

Interpretation of the OCIO standard

"Abbreviated summary of that IT Asset Disposal Standard" for Smart Devices such as Smart phones and tablets. Note these are described in the standard as storage media.

> "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)."

OCIO Statement:
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.

Statement Interpretation:
1. Smart Devices unlike workstations are not considered assets as they are under $1000.00 in value. As such, the same type of documentation collected now for the destruction of Blackberrys and cellular phones would be collected for smart devices.

New smart devices are not assigned asset tags. The Mobile Device Access Service (MDAS) does not require the serial number or other pertinent details regarding the device to connect it to the service. Future tools may provide reports that allow MDAS to collect this information while the device is connected to the service; however, these reports are only available while the device is connected.

Original information created on the device must be managed following information lifecycle practices and is the responsibility of the device user. If the device is accessing Government email contacts and calendar information using the OCIO Mobile Device Access Service then this information is stored securely on the servers and is not considered original to the device. Emails using the service or meeting and contact information may be created on the device and it will be synchronized with the server. For information retention purposes, information stored on the server is the primary source. An example of original information created on the device and not synchronized back to the server could be a document created within a word processing application resident on the device.

OCIO Statement continued:

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

b) Encryption of the storage device and subsequent data erasure with either:

- a single pass overwrite solution, or;
- ☑ deletion of the encryption key for devices that were encrypted using government standard.

Statement Interpretation:

2b ☑. Deletion of the encryption key for devices that were encrypted using government standard applies to all Government owned and approved Smart Devices (phones and tablets). Once the phone has been reset to factory settings, the encryption key is deleted.

Smart phones and tablets that have been sanctioned for Government use must meet certain security standards. The minimum standards are as follows:

- Must be either HW encrypted or capable of SW Encryption including any SD cards
- Must be capable of remote and auto self-wipe after a set number of failed attempts
- Must have a device password lock and be set to autolock after a set timeframe.

OCIO Statement continued:

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, warranty and disposal are defined in the Disposal Handbook."

Statement Interpretation:

3. Each Ministry or Broader Public Sector organization using AIR's services are responsible for ensuring devices are ready for resale. Devices are to be wiped to factory settings prior to being sent to AIR for resale or destruction. Devices that have not been wiped to factory settings may possibly be returned to the sending organization or may be wiped by AIR.

The current form that is used to send devices to AIR for destruction may be used for devices sent to AIR for resale. The form is generally completed for each bundle of devices contained in a larger box and is found at https://assetdisposal.gov.bc.ca/ (If you have not used this site before you will need to send an email with your IDIR name to the Surplus Mailbox).

Mobile Device Disposal Interpretation and Guidance Document

Mobile Device Disposal Checklist

- Ministries are to work with device users to ensure the devices have been wiped to factory settings by the device user.
- If devices cannot be wiped, or if they are in obvious disrepair, they are to be collected separately and sent for shredding by AIR.
- AIR, will review and determine which devices are suitable for resale.
- AIR can also perform a wipe to factory settings if this is not already completed for a device received in the warehouse.
- When replacing a device, the Ministry should provide instructions to the device user pertaining to their old device to inform them of their responsibilities.
    - 1. Turn off any features such as "find my iPhone" that may interfere with a password reset
    - 2. Reset the device to factory settings before they return the old device for disposal or redistribution.
- Ministries will continue to collect devices from the end users as they do now. Ministries that collect devices centrally may continue to fill out one form that covers all the devices located at https://assetdisposal.gov.bc.ca/ (If you have not used this site before you will need to send an email with your IDIR name to the Surplus Mailbox).

The minimum required for a resale device is the device itself. Cables and a box would be preferred; however cables are readily available from retail stores. Devices without cables will have a diminished resale value.

If excess cables are received, they will be first matched up with devices and any additional cables could be sold separately. Accessories returned in good condition would be welcomed for resale.

Note: for iOS devices that have the "find my iPad" or iPhone feature turned on, and where the passcode is unknown and unobtainable, these devices will be shredded. The exception might be if there is significant value to the device and receipts are available, then the device may be restored by Apple. This is labour intensive and is only valuable for near new devices.