CMSGu2015-05

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Secure Disposal of Information

CERT-MU

National Computer Board
Mauritius

September 2015

Issue No. 5

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide a knowledge-based framework which will help maintain best practices regarding information asset disposal within organisations.

1.2 Audience

The target audience for this document include all organisations that make use of information and information systems to store and process information.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on information handling, including information disposal.

Section 3 shows the threats to the information destruction process.

Section 4 gives details on the secure disposal of Information Systems.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

2.0 Background

Information disclosure has become a major risk to organisations working with sensitive data, predominantly due to the increasing dependence on information storage systems and the use of disposable media.

Information storage systems or assets include media that are used to store, transport or backup information. Storage media can be hard drives, tapes, portable storage devices, CD/DVD/floppy disks and other electronic storage media. When disposing of information storage assets special procedures must be followed to ensure information has been removed prior to disposal. The information may be sensitive or personal and there may be legal, policy or program requirements for keeping it confidential and secure.

Establishing and communicating specific rules for information handling during the asset disposal or transfer process is necessary to increase the certainty that information is managed correctly and is not inadvertently disclosed. There may also be cases where the information must be preserved rather than destroyed. Situations where consideration of disposal of assets that store information include: hardware refresh cycles, replacement of broken equipment, relocating or closing of an office location, organizational changes, and at the end of the scheduled information life cycle.

3.0 What are the threats to the information destruction process?

Threats to the destruction process can range from forcible attack to more sophisticated surreptitious methods and can occur before, during or after the destruction process. For example:

- Accidental loss;
- Emergency abandonment (individual, vehicle or building);
- Espionage (commercial or state sponsored);
- Hijack or vehicle theft (from site or during transportation);
- Insider attack (e.g. disgruntled employees or investigative journalists);
- Theft (from site, vehicle, storage or destruction facility).

3.1 Areas of concern

The major issue regarding disposal of information storage assets is correctly managing the information stored on the asset prior to disposal.

There are two primary concerns:

1. Information may be left on the storage device after it leaves government control, and is later retrieved and exploited by unauthorized personnel, and
2. Information which should be retained as a primary record is lost when the storage device is disposed of.

Many factors amplify these concerns:

- Where inventories of information are inaccurate or incomplete, it will be difficult to determine storage requirements, or what level of sensitivity the information has and may result in inappropriate storage or disposal.
- When information management procedures are manual or complex the information sensitivity maybe unknown, unclassified or classified incorrectly resulting in inappropriate storage or disposal.
- Small storage devices can retain vast quantities of information and can be easily lost and result in the exposure of sensitive or personal information.
- Many organizations are involved in the lifecycle of information assets and where best practices and procedures for asset management are not in place it can result in security or privacy breaches.

3.2 Mitigating the risk of sensitive information breach

Based on the structured assessment of the need, a number of options should be considered to achieve the desired balance between security and operational effectiveness. For example:

- Confirm the highest level of protective marking or sensitivity of information to be disposed;
- Identify the type of storage media – the type of media will determine the most suitable methods of destruction;
- Storage of sensitive assets – on-site will require storage in a suitably secure location. Off-site will also require secure storage; service providers should inform customers if secure storage is available and to what level;
- Method of destruction – a number of options are available with specific advantages and drawbacks that should be matched to the project operational requirements;
- Location of destruction facilities – on-site will require either the purchase or hire of approved destruction equipment, or contracting of an approved service provider with a mobile destruction facility. Off-site will require the support of an approved service provider;
- Transportation – consider appropriate communication, handling in transit procedures, manning level, vehicle tracking etc.;
- Personal escort and/or witnessing of physical destruction – can provide an extra level of confidence but will also require staff time;
- Vetting – all those involved in the disposal process should be vetted to the appropriate level;
- Audit trail and records keeping – provide confirmation and assurance that material has been disposed of according to the agreed requirements.

4.0 Secure Disposal of Information Systems

4.1 Disposal of computer system containing sensitive data

- When disposing of a computer system, you need to address the following:
  - Data: you must delete all sensitive data on the system before disposal.
  - Operating System & Copyrighted Applications: you must delete all copyrighted software applications other than the original operating system. If you have upgraded the original operating system, you must revert to the original.
  - Hardware: this can either be taken away and destroyed, or recycled, subject to the points above.

4.2 Deleting sensitive data irrecoverably

- When computer systems are disposed of, the custodian has a duty of care to ensure that any sensitive data on the system is also safely destroyed, so that it cannot be recovered and used for unauthorised purposes.
- Special measures should be taken, where the system contains data of the following types:
  - Patient-related data, including "coded" data
  - Commercially sensitive research data
  - Financial data
  - Personal data of any other type (i.e. data covered by the Mauritian Data Protection Act 1997)
  - In these cases, the data should be destroyed before the computer system is discarded.

4.3 Deletion of data

- Warning: simply formatting the hard drives on a modern computer system does not prevent files which are deleted from being accessed by later inspection of the disk, using data recovery software. Do not rely on disk formatting.
- There are a number of software products available, which ensure secure deletion of data on your computer. They work by overwriting the data on the system many times, ensuring that nothing can be recovered.

4.4 Hardware destruction

- If you do not wish to undertake the destruction of the data yourself, you can have the system, or its hard drives physically destroyed. There are a number of firms that specialise in secure destruction, who will collect your computer system, and ensure all data on the system is destroyed.
- Once you have deleted all the data on the disk using methods such as overwriting, degaussing or physical destruction, there are a number of options for final disposal of the computer system.

4.5 Deleting the Operating System and copyrighted applications

- When disposing of a computer system for re-use it may only contain the original licensed operating system provided when it was purchased. If you are unable to do this, then you should remove the operating system completely. Software applications should be securely deleted in accordance with the vendor's instructions.
- If the operating system is a Microsoft product, you must revert to the Microsoft operating system supplied with it at the time of purchase. If you do decide to this, you must include all the media, and the Microsoft Certificate of Authenticity supplied with the system.
- All other data and applications must be securely deleted using the abovementioned techniques.

4.6 Disposal of computer systems

- Any computer systems in working order which are donated or sold to a third party must be subject to electrical Portable Appliance Testing (PAT), prior to any change of ownership.
- When you are confident that you have securely deleted any sensitive data your computer system may once have held, then there are several options for its final disposal, for instance discard or sell it.

5.0 Conclusion

The traditional deletion of files does not permanently remove data from a storage device. In fact, it just instructs the computer that the old data sectors are now available to be overwritten. The old data remains in place and is thus a major security risk. As a result, it is imperative that information asset disposal should be done using a formal data removal process approved by Information Security to securely delete data.

6.0 References

- **http://systems.hscic.gov.uk**
- **http://www.cio.gov.bc.ca**
- **https://computerservices.temple.edu**
- **https://www.priv.gc.ca**
- **http://its.yale.edu**
- **http://www.cpni.gov.uk**
- **https://www.imperial.ac.uk**