Media Handling Procedure

Ncell

Procedure

Approved Date:- 07/09/2016

	Ncell	Classification: Internal
	Media Handling Procedure	Owner: CIO/Head of IT
		Effective Date: 07-09-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Procedure Name DOCID: PR-IT-IS-04

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-04 Media Handling Procedure**
Effective Date:	7th September, 2016
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
External Auditor (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Ncell Employees and External Auditor (If required)

iv. Digital Signature

CEO	CIO/Head Of IT

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	07-09-2016	Information Security Team	Initial document	Simon Perkin	07-09-2016
1	15-09-2019	Information Security Team	Revised – Formatted the document, added description for DLP use.	Vishal Mani Upadhyay	13-12-2019
2	13-12-2019	Information Security Team	Revised Approval	Andy Chong	17-12-2019
3	20-10-2021	Information Security Team	Added 5.3 Physical Destruction "In other cases, if hard drives which stored sensitive information needs to be scrapped, it might not be enough to wipe the data."	Vishal Mani Upadhyay	19-12-2021
4	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
5	28-09-2023	Information Security Team	Review and Updating – Period changed from annual to once every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
6	27-12-2023	Tarani Prasad Chaudhary	Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
7	25-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Table of Contents

1. Purpose

This document aims to provide a clear set of procedures for handling of media devices and paper documents to ensure that:

i. All authorized users of IT assets and IT media are fully aware of their obligations towards media disposal;
ii. Intentional/ unintentional leakage of information from discarded media is reduced;
iii. Information disposed using this procedure, cannot be retrieved using retrieval/ computer forensic tools;
iv. Only intended information or intended media has been erased/ wiped off; and
v. Steps are identified which must be taken to reduce the risks associated with the use of removable storage devices.

2. Review and Updating

This Standard Operation Procedure to be reviewed once in every two years and whenever significant changes occur in the organization.

3. Scope

The scope of this procedure is applicable to all assets containing Ncell's information. Additionally, the media disposal process is not applicable for faulty equipment being sent out of premises for repair.

4. Responsibilities

4.1 Media Disposal

Type of Media	Responsibility
Hardware/Software Disposal (e.g. hard disk drives contained in servers/storage systems, backup tapes etc.	System owners, where applicable or OS / Database Planning Team
Paper Assets	End users
Laptop/PCs	IT Service Desk / Help Desk

4.2 Removable Media Management

4.2.1. Information Security Team

Information Security Team shall:

i. Monitor flow of information through USB ports on all Ncell-owned laptops/desktops through the organisation's DLP solution.
ii. Analyse events triggered through the DLP solution and log it as an information security incident if found genuine.

4.2.2. End Users

In case portable devices are approved to be used, users must:

i. Not use removable storage devices for primary storage of any data;
ii. Shall not copy customer/subscriber data or secret/confidential Ncell information without the consent of the unit head;
iii. Scan the removable media device for any malwares prior to utilizing them for transfer of data.
iv. Be responsible for the security of their removable media device.
v. Removable Media should always be in possession of an authorized person; and
vi. Immediately report to the Information Security Team of any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

4.2.3. Unit/Section Head

Unit/ Section Head reserve the right to ban the use of removable media device at any time as protection of data is the highest priority.

4.2.4. Information Security Team

The Information Security Team must:

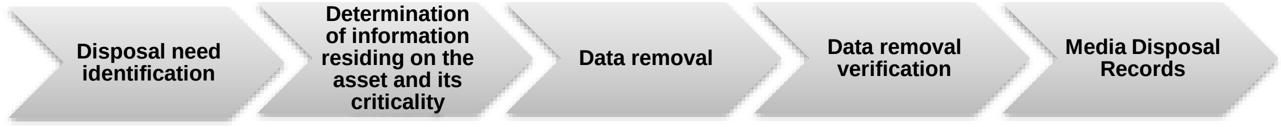
i. Revoke access to removable devices in case of information security breach;

ii. Revoke access to removable devices in case the device found to be infected with a virus.

The Information Security Team reserves the right to refuse the ability to connect removable media devices to corporate and corporate-connected infrastructure if it feels such equipment is being used in such a way that puts the organization's systems, data, users, and customers at risk.

5. Media Disposal Process

Media disposal process is conducted in the following phases:



Disposal need identification

Determination of information residing on the asset and its criticality

Data removal

Data removal verification

Media Disposal Records

5.1 Disposal need identification

The first step in disposal process is to identify when the asset (hardware/ paper) needs to be disposed. The need for disposal may be triggered by the following scenarios–

i. When asset is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held.

ii. When the asset is redundant and hence no longer in use.

iii. When the asset has exceeded its warranty/ retention period; and/ or

iv. When the asset has malfunctioned and cannot be repaired.

5.2 Determination of information residing on the asset and its criticality

The security classification for the information assets is determined during the asset criticality identification phase. Referring to this classification, the system owner shall design a disposal process that will ensure adequate protection of the media's information.

5.3 Data Removal

Once it has been decided to dispose of information on media devices/ paper, then the following techniques can be used as a reference of recommended techniques to accomplish the job.

Wiping programs

i. Wiping of data means to completely erase data from memory or the hard disk. Normally, when a disk file is deleted, only the file name in the directory is marked as deleted, but the data still resides in the disk sectors until overwritten by new data later on by the same or some other application.

ii. Wiping is a process of overwriting the space where files are located with random data. For maximum security, random data should be written into the sectors several times, because forensic analysis can detect the previous magnetic residue if the magnetic bits are overwritten only once. In addition, caches should also be cleared.

Physical destruction

Certain media can be read many times but can only be written once. These media cannot be overwritten. Sometimes the media are defective and can no longer be used for retrieval or storage. In other cases, if hard drives which stored sensitive information needs to be scrapped, it might not be enough to wipe the data. In each of these cases, the media should be physically destroyed through burning, crushing or smashing.

Shredding

This is a mechanical method of cutting paper into chad, typically either strips or fine particles to completely destroy hard copy documents. In the absence of a shredding machine, the user can manually rip the document into pieces such that it cannot be put back together.

Based on the criticality of information stored, the following media disposal strategy should be considered for each information type –

Information Type	Information Classification			
	Secret	Confidential	Internal	Public
Solid state storage media such as USB flash drives, Solid state and hybrid hard drives, Secure Digital cards	Overwrite the entire media with wipe tools	Overwrite the entire media with wipe tools	Delete files	No special requirements
Optical storage media such as CDs, DVDs	Shred media	Physically destroy the device	Physically destroy the device	Physically destroy the device
Removable magnetic storage such as Floppy disks, Tape Drive Media	Shred media after degaussing	Physically destroy the device	Physically destroy the device	Physically destroy the device
Duplication equipment such as copy machines, fax machines, printers, etc.	Perform a full manufacturer’s reset to reset the machine to its factory default settings	Perform a full manufacturer’s reset to reset the machine to its factory default settings	Delete files	No special requirements
Networking Devices such as routers, switches, hubs, MSC, BSC etc	Perform a full manufacturer’s reset to restore the networking device back to the factory default settings.	Perform a full manufacturer’s reset to restore the networking device back to the factory default settings.	Delete files	No special requirements
Hard copy information	Shred the data	Shred the data	Shred or tear all documents and files, or place in secure receptacle for future shredding	No special requirements

5.4 Data Removal Verification

Post completion of media processing, verification of the process must be conducted by independent personnel to ensure that all critical information has been removed or securely overwritten. If any files or fragments of files are evident on the media at this stage, then data removal has been unsuccessful. In this case, the process of media disposal shall be repeated by using a greater number of passes or consider using a different technique altogether.

5.5 Media Disposal Records

It is critical that Ncell maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media. This is to ensure that management officials are included in documenting the media sanitization process for establishing proper accountability of equipment and inventory control.
The following information should be captured –

i. Type of media and its details
ii. Information/ data classification in the media
iii. Disposal method

6. Reuse of Media

i. When servers are re-allocated for different purposes / projects, internal hard disks shall be wiped as per section 5.3.
ii. Storage provided by SAN shall be sanitized using suitable process as per section 5.3 before
iii. reallocation for different purpose / projects.
iv. Laptops hard-disk data shall be wiped as per section 5.3 before allocating to another employee or personalizing the laptop (handing ownership of the laptop to the user).
v. Hard disks returned to vendor for warranty / support purposes shall be wiped as per section 5.3 before handing over to the vendor.

7. Governance and Compliance

i. All Ncell employees / users that do not adhere to these guidelines for any account may be subjected to disciplinary action.
ii. Exception management process shall be followed to raise exceptions for this procedure.
iii. Internal and external compliance review shall be conducted as per the organization’s internal and external audit requirements.

8. Associated Documents

i. Asset Management Procedure