एन एम डी सी
NMDC

MEDIA HANDLING POLICY

Author		**Document name**		**Date of first issue**	
Owner	C & IT Department	**Document ref. no.**		**Date of latest re-issue**	
Version	1.1	**Page**	1 of 10	**Date of next review**	
Issue Status	Under Review/ Live	**Security classification**	Internal use only	**Reviewer**	

एन एम डी सी
NMDC

MEDIA HANDLING POLICY

VERSION CONTROL

Revision no.	Date of issue	Prepared by	Reviewed by	Approved by	Issued by	Remarks

एन एम डी सी
NMDC

MEDIA HANDLING POLICY

OBJECTIVE

The objective of this policy is to protect safeguard the media against disclosure, theft, or damage and to inform how to handle different media types and events in the media lifecycle with proper media labeling, storage, transport, and disposal and to log, and securely store media.

SCOPE

This policy is applicable to NMDC users and internal IT systems. Computer media includes tapes, disks, USB, Hard Disk, CD, DVDs, pen-drives etc.

POLICY RULES

1. Security Executive assigned for the protection physical assets and media are responsible for ensuring physical security of the media.
2. Group Leaders authorize for media to be removed from the company and a record of all such removals to maintain an audit trail should be kept.
3. If no longer required, the previous content of any re-usable media that is to be removed from the company should be deleted by formatting.
4. External media such as USB Drives, Hard disks, CDs, etc. should be allowed only from authorized stations.
5. Use of only identified and trusted media shall be allowed on devices on the network.

Commented [BA1]: Department to decide whether to retain this point or remove it

New Media

1. One should always inspect new media for damage and verify that it is in good working order before use and do not contain preloaded Viruses/Spyware
2. When the media is used to store or transfer sensitive information, it should be labeled and properly stored.

Commented [BA2]: Labelling- all media to have company name/logo printed

Media Storage

1. The media containing sensitive or restricted information must be stored securely within a locked container, office, or suite and in accordance with manufacturers' specifications.
2. All media should be handled with care and it should be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution.

Media Transfer

Media used to transfer sensitive information between devices or between individuals, whether local or remote, should be handled with following guidelines:

Transfer between devices:

1. Users should log the transfer to record the change in location to transfer information to another computing device.

MEDIA HANDLING POLICY

2. If a memory stick is used to transfer working files from user desktop to laptop, no logging is necessary. If media is used to transfer large volumes of information/data to alternate information systems, the same shall be logged and the media (CDROM or other permanent media) shall be labeled.

Commented [BA3]: Log to be maintained with details of which media taken, when, by which department, and for what purpose

Following guidelines are to be followed for media in transit:

1. Reliable transport or agency is used. A list of authorized agency as agreed with management and a procedure to check the identification of couriers shall be implemented.
2. Packaging is to be adequate to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
3. Special controls are adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, Tamper evident packaging (which reveals any attempt to gain access), encryption of data etc.

Disposal of media

1. Media should be disposed-off securely and safely when no longer required because sensitive information may be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media should be established to minimize this risk.
2. Media containing sensitive information is stored and disposed-off securely and safely, e.g. by incineration or shredding, or formatted before use by another application within the organization.
3. When accumulating media for disposal, consideration is given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.
4. Disposal is a special case since the asset requires any company sensitive data removed prior to disposal. For any data storage devices, the manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Some of the actions and process that shall be followed for the device based on data sensitivity according to the data assessment process are:
   a) None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
   b) Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
   c) Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
   d) High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
5. The following list identifies items that require secure disposal:
   a) Paper documents;
   b) Voice or other recordings;
   c) Output reports;
   d) DAT tapes;
   e) LTO tapes;
   f) Removable disks;
   g) Optical storage media (all forms and including all manufacturer software distribution media);
   h) Memory stick;

i) Hard drives;
j) Program listings;
k) Test data;
l) System documentation.

6. Approved technologies are to be specified in a Media Data Removal Procedure document by asset type.

Security of Electronic Office Equipment

Electronic office equipment includes faxes, printers, scanners etc.. These need to be physically secured, as they are sources of receipt or processing of data in a physical or voice format. The security considerations are as follows:

1. The faxes and printers are placed in a secured area. Access to both is restricted to ensure that no visitor can gain easy access without notice of the staff. Security Executive for the fax and printer should ensure the physical access security and take necessary precautions. They should be protected from heat, pollution and other environmental hazards.

Clear Desk & Clear Screen

The company should follow a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours. The following controls should be implemented:

1. Paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
2. Sensitive or critical business information should be locked away (ideally in a fire resistant safe or cabinet) when not required, especially when the office is vacated.
3. The users should lock personal computers/ laptops when left unattended.
4. Photocopiers are to be locked (or protected from unauthorized use in some other way) outside normal working hours.
5. Sensitive or classified information, when printed, is to be cleared from printers immediately.

Insurance

All IT Assets must have sufficient insurance coverage against fire, theft, arson, rioting, etc.