एन एम डी सी

NMDC

ASSET MANAGEMENT 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

ASSET MANAGEMENT POLICY

VERSION CONTROL

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

एन एम डी सी
NMDC

ASSET MANAGEMENT POLICY

OBJECTIVE

An IT Asset is any company owned information, system or hardware that is used in the course of its business activities. The objective of this policy is to protect & control data integrity, computer systems and organizational IT assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. Additionally, this policy will define the guidelines for physical as well as data security on desktops and laptops.

SCOPE

The policy is applicable to all NMDC's IT assets which include but are not limited to:

1. Computing devices (Desktops, laptops, tablets, smartphones, LCD/Flat screens, palmtops etc.)
2. Output devices (printers, CD/DVD etc.)
3. Input devices (Scanners, CD/DVD writer etc.)
4. Servers
5. Application software
6. Storage devices
7. Network and communication applications

IT assets should not be confused with nor tracked with other organizational assets such as furniture.

This policy applies to all company users, contractors, trainees and clients working in NMDC premises.

POLICY RULES

Asset purchase and acquisition

1. IT purchases shall be based on business need.
2. The C&IT dept. or business unit shall initiate purchase of any IT asset.
3. Any asset acquisition initiated by business unit shall be approved by the business unit head as per the grants of authority with the recommendation of the C&IT department.
4. The purchasing department shall seek, where required, inputs from the C&IT department in finalizing the list of vendors for IT assets.
5. In case of recurring purchases of a similar asset, the purchasing department shall conduct procurement based on standardized technology guidelines as provided by C&IT Department from time to time.
6. Any asset purchase and acquisition contract shall be awarded after following vendor evaluation and selection processes.
7. The vendor evaluation shall be based on (but not limited to) response to RFP/RFQ/RFI, vendor reference, site visits, post- sales support, technical capability, pricing, product quality, comparative analysis between vendors, market intelligence, etc.
8. Procurement of software licenses shall be based on NMDC's software control policy.

9. Financial approval for procurement of IT assets shall be as provided in the financial delegation of powers as prescribed by the finance department from time to time.
10. All records of acquisition shall be retained for future reference.

Asset ownership and use

1. The ownership of the IT assets shall be vested with the IT department while the custodians of the IT assets shall be
   a) Individuals in the case of all personal IT assets like desktops, laptops, personal printer, personal scanners etc.
   b) Admin/ Security in-charge in the case of network printers and common IT equipment like network switches, routers etc.
2. The IT assets provided to individuals shall be for business/official use only (except for BYOD devices)
3. In case of asset replacement, old assets should be returned to the IT Department/Central Store immediately after the new asset has been provided.
4. Assets in IT department shall be re-issued to new users and the details of the same must be recorded.
5. C&IT department shall technically review the latest configuration/technology of laptops/desktops on a periodic basis and recommend a standard configuration to the procurement department. The C&IT Department can approve any deviation to the standard configuration based on the business need and vendor recommendations.
6. Security audits should be performed internally on a regular basis to ensure compliance with the standard requirements.
7. The user/user's department/local administration (depending on the case)/custodian shall be responsible in the event of misplacement or theft of any IT Asset.
8. Only licensed and approved software should be installed on IT assets.
9. Periodic review shall be carried out by the C&IT department to verify and validate the usage of licensed software.
10. The C&IT department shall have all rights to track and verify the configuration of the hardware and software of the IT asset for the purpose of audit and/or maintenance activities.
11. The IT assets shall be insured as per the insurance requirements of NMDC.

Asset allocation

1. **Laptop/BYOD allocation**
   Allocation of laptops to NMDC's employees shall be based on business need and laptops shall be allocated to all employees whose work level is E1 and above. For all the other employees, allocation shall be based on business need with the approval of the Corporate IT head.
2. **Desktop allocation**
   Allocation of desktops to employees shall be based on business need and desktops shall be allocated with approval from the business unit head.
3. **All other peripheral devices allocation**
   Allocation of other peripheral devices shall be done with the approval of the Corporate IT head.

एन एम डी सी
NMDC

ASSET MANAGEMENT POLICY

Asset classification and labelling

1. All IT assets shall be classified into the following broad categories for the purpose of grouping (based on homogeneity), identification and tracking
   a) Computing devices (laptops, desktops, tablets, smartphones)
   b) Servers
   c) Printers
   d) Application software
   e) System software
   f) Networking and telecommunications
   g) Security
   h) Power systems
   i) Computer Accessories
2. The IT assets (excluding software) shall be uniquely numbered and inventoried or identified bar codes in the asset database maintained by the C&IT department and labelled for identification and verification. Access to the asset database shall be restricted to limited people in the C&IT department with prior approval of the Corporate IT Head.
3. Asset verification for IT assets shall be conducted annually to verify the existence and custodian of asset.
4. The software IT assets (the original software CDs/DVDs etc.) shall be maintained by the C&IT Department and inventoried in the asset database and the software register indicating the deployment of the software.

Asset upgrade

1. Assets (computing devices) shall not be upgraded within 4 years of procurement, unless approved by the Corporate IT Head based on business and applications need.
2. Software upgrade shall be carried out based on application requirements and support considerations.
3. Asset database shall be updated with the upgrade details by the C&IT Department.

Updates on Assets

1. Before approving updates, administrators should know:
   a) The addressed vulnerability
   b) What previous patches are required or what system update is required
   c) What programs are affected by the change
   d) What may be broken by the change
   e) How to undo the change
2. It is recommended that new patches be tested in a controlled environment that mimics the infrastructure of the production environment before patches are applied
3. Each server should have documentation including a list of applications running on it and a patch history.
4. All patches approved and pushed on user desktops/laptops should be documented/ logged.
5. An authorized system administrator shall review available updates weekly.

एन एम डी सी
NMDC

ASSET MANAGEMENT POLICY

Transfer of assets

1. Transfer of desktops from one user to another user or from one location to another location or business unit shall be carried out with the approval of the C&IT Department.
2. Transfer of assets such as servers, networking and telecom assets, security and power systems shall be carried out only upon prior approval of the C&IT Department.
3. The asset database shall be updated in all cases of transfer of assets by the C&IT Department. Also, where necessary, C&IT Department shall update other documentations such as Network Diagrams. Telecom Diagrams etc.

Retrieval of assets

1. Assets shall be retrieved from the employees/temporary hire/third party etc. in case of employee separation or on providing a new asset in place of an existing asset or end of temporary asset requirement.
2. The asset database shall be updated in all such cases
3. The C&IT department shall inspect the asset at the time of retrieval for any damage. In case of damage identified by the C&IT Department, as due to negligence/improper use by such user, the C&IT Department shall recover, from such employee/temporary hire/third party an appropriate residual amount, for such damages, after considering warranty/insurance cover for such asset.

Asset retirement and disposal

1. The C&IT Department shall retire the IT assets (desktops/laptops) from use, based on the company's approved asset retirement timeframe. The Corporate IT Head, on a case-to-case basis determines the retirement of all other IT assets
2. The C&IT department may decide to retire the assets before the life period of the asset for some special reasons such as but not limited to:
   a) Technology obsolescence
   b) Defective hardware
   c) Prohibitive cost of maintenance
   d) Damaged or irreparable condition
3. The IT assets for disposal shall be cleansed of any specific license/proprietary software and data by the C&IT department
4. The retired assets, after removal of company data, may be disposed in any one of the following ways as decided by the C&IT Department
   a) Donation to charitable/ other institutions
   b) Auctioned/distributed/sold to employees
   c) Sold to third parties
5. In case the disposed asset needs to be destroyed, the IT Department shall follow the E-waste management, handling and disposal policy.

Installation qualification

1. System and Infrastructure team shall be responsible for ensuring the installation qualification process.

2. The installation qualification process shall:
    a) Confirm that the system specifications meet the user requirement specification
    b) Conform to the manufacturer's technical description and installation requirements
    c) Confirm that appropriate documents exist to enable the system to be operated and maintained safely, effectively and consistently
    d) Ensure that all required system software and server support application software are provided
    e) Ensure that the backup software or devices required are properly installed for backup
    f) Ensure that the system is in satisfactory condition for the Operational Qualification to be started
3. The installation qualification test shall be recorded
4. All installation qualification reports shall be submitted to the Head of System and Infrastructure team for review
5. The installation qualification process shall not be applicable in certain cases (personal devices)

Operational qualification

1. The System and Infrastructure team shall ensure operational qualification is being performed for IT systems before going into production environment.
2. The operational qualification testing shall:
    a) Verify the operational aspects of the server that are deemed critical to its satisfactory performance
    b) Ensure that adequate security controls are in place as per the security best practices of the component
    c) Ensure that system can produce the required level of performance through stress/load testing
    d) Ensure that the systems have the required level of capacity
3. The operational qualification team will have members from:

Desktop and laptop security

6. Each desktop/laptop should be secured with a login and password. The password should satisfy NMDC's authentication policy. No passwords should be stored in clear text on the system. Also, the "Remember Password" option prompted on desktops/laptops shall not be used and shall be kept disabled.
7. Administrator password should be kept with IT administrator.
8. Suitable screen saver and wall paper relevant to the organization will be pushed to all official desktops/laptops along with a screen lock that engages after the keyboard and/or the mouse have been idle for a period of 30 minutes.
9. Each desktop/laptop should be turned off when not in use for an extended period of time or should be powered down into a suspended status, except as specifically authorized by the security administrator.
10. Anti-virus software approved by the C&IT Department only should be installed and be active on each desktop/laptop. Designated staff should make certain that the desktop has the most current anti-virus updates and appropriate patches installed. The program shall be configured for real

time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once a week.

11. Desktops/laptops that contain confidential information and/or are assigned to system administrators, should be configured so that they cannot be booted from USB, floppy disk or CD ROM.
12. Folders should not be shared unless absolutely necessary
13. Root directory should not be shared at all with other desktops/laptops in the network.
14. No modems or broadband connectivity should be used in desktop computers.
15. If the computer is owned by the organization and has been returned from a period when an employee has used it during tour/official duty, the following check shall be performed.
    a) Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. (If it fails one of these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computer can be used in the building).
    b) Scan for additional malware such as adware or spyware shall be done to ensure that the desktop is free from virus worms, etc. Remove any malware on the computer if any was detected and log information if any malware, vulnerability is found.
16. All desktops shall be company provided Microsoft Windows versions. Exceptional approvals to be taken for other OS.
17. Desktop/laptop updates may be done using company provided tools depending on the type of desktops/laptops and their operating systems. System update server installed internally by the company will save time and expense since all systems may be updated from one server at the same time.

User responsibilities

1. Users are expected to use computer and network resources in a responsible manner. Users should take appropriate precautions to ensure the security of their passwords and prevent others from obtaining access to their IT assets.
2. Convenience of file or printer sharing is not a sufficient reason for sharing computer accounts and shall be restricted in order to avoid spread of virus in the network.
3. Users may not encroach on other users computer resources for actions that include, but are not limited to, tying up computer resources with trivial applications or excessive game playing, sending frivolous or excessive messages, including chain letters, junk mail, and other similar types of broadcast messages, or using excessive amounts of storage.
4. Critical data files should be regularly backed up by the users.
5. All users who process sensitive business related information on their personal computers must ensure that these computers provide adequate and appropriate security for that information. This includes:
    a) Disabling unencrypted wireless access;
    b) The maintenance of adequate physical security;
    c) The use of anti-virus and spyware software; and
6. The following are prohibited while using company IT resources, including computers and networks owned by NMDC/hired from Service Providers.
    a) Modifying system or network facilities, or attempting to crash systems or networks.

b) Using, duplicating or transmitting copyrighted material without first obtaining the owner's permission, in any way that may reasonably be expected to constitute an infringement, or that exceeds the scope of a license, or violates other contracts
c) Tampering with software protections or restrictions placed on computer applications or files.
d) Using NMDC's IT assets for personal profit purposes
e) Sending messages that are malicious or that are found to be harassing other users/colleagues.
f) To obtain unauthorized access to records, data, and other forms of information owned, used, possessed by, or pertaining to the Company or individuals.
g) Accessing another person's computer account without permission or by spoofing. (Users may not supply false or misleading data, or improperly obtain another's password to gain access to computers or network systems, data or information. Obtaining access to an account name or password through the negligence of another user is considered to be a specifically prohibited use).
h) Intentionally introducing computer viruses, worms, Trojan Horses, or other rogue programs into IT assets that belong to, are licensed, or are leased by NMDC.
i) Physically damaging IT assets
j) Using, or encouraging others to use, IT assets in any manner that would violate this or other NMDC policies.

7. Laptop users will have the following responsibilities:
   a) Make a note of the model, make and serial number of the laptop allocated to individual for future reference
   b) Ensure from issuing authority/Personnel Head that the Laptop issued/in-use is covered under Insurance/Transit-Insurance.
   c) While not in use, user should keep laptop secured in its docking station/locked cabinet or locked to the desk of the office
   d) Refrain from giving laptops to someone else either for business or nonbusiness usage. In case of a need to share a laptop, user should ensure that confidential information on the laptop is password protected
   e) While on travel, user should keep the laptop under constant surveillance
   f) Exercise caution while using Internet service outside NMDC premises/network using the laptop
   g) Refrain from reading or replying to sensitive mails from public places such as airports, meeting rooms. In case of absolute need, one should ensure others are not watching laptop screen
8. Usage of assets should be consistent with the NMDC's code of conduct, and Information Technology Act 2000 (and amendments to it).