एन एम डी सी

NMDC

PHYSICAL ACCESS SECURITY 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

PHYSICAL ACCESS SECURITY POLICY

VERSION CONTROL

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

एन एम डी सी
NMDC

PHYSICAL ACCESS SECURITY POLICY

OBJECTIVE

This document establishes the operational standard for the physical security of sensitive information and IT assets.

SCOPE

The policy applies to NMDC`s Information assets, employees, visitors, vendors, third parties working in the premises and in possession of the company's IT assets and requires that all NMDC`s Information technology assets are physically secured from unauthorized or illegal access as well as from business and environmental threats.

RESPONSIBILITY

The IT Security Nodal Officer is primarily responsible for execution of the procedures for ensuring physical security of IT resources. Personnel, Admin, IT communication department are responsible for supporting IT Security Nodal Officer to achieve this task.

All employees, third parties and temporary hires have to adhere to the company policy for physical security.

POLICY RULES

Entry restrictions

Entry restrictions for premises

1. All the employees of NMDC should be provided with proximity\ swipe cards, which have their photographs on them. Visitors should sign in the register (kept for visitors) with visitor's name, signature and time of entry.
2. Human Resources should access the logs from the access management software for employees.

Entry restriction for visitors

NMDC should identify areas where outsiders should not be permitted to enter unless the following are done:

1. Visitors should be classified into vendors, suppliers, site-visitors, contractors, consultants, auditors and government officials.
2. The regular vendors, suppliers should be listed in independent registers and security personnel should validate their name and identity before allowing them entry into premises. These parties should be assigned semi-permanent passes or identification badges by the security department.
3. Visitors should sign-in, in the visitors' logbook, which should be kept with the security guard. This should be retained and reviewed every day.
4. Employees should intimate the security personnel of the expected visitors in advance. The security personnel should, in turn, inform the concerned employee about the arrival of the visitor in the office.
5. Visitors should wear a visitor badge to inform personnel that a non-employee is in the area.

6. Gate pass should be issued to effect removal of NMDC's property from the building.
7. The returnable gate-passes not received within a month should be reported to concerned head of the department.
8. Visitors should obtain prior written permission from Administration department to work on weekends and holidays.

Entry restrictions within premises

Entry within premises is restricted based on the role of the employees. The employees in corporate functions (e.g. HR/Admin, Accounts, Finance, etc.) should have access to all the areas except electric panel/EPABX, server room and communications room. Server and communication room access should be limited to the C&IT Department. The restriction should be enforced through use of electronic locks with access through proximity / swipe cards.

Access to server room

1. The access to server room should be restricted by the electronic locking system, which opens by proximity/ swipe cards. The access is granted only to specified employees of C&IT Department. Security Officer should authorize the access respectively.
2. Security Officer should review the logs on a random basis, at least once a month. The reviews are done to check the accesses to the server room.
3. Vendors need to access the server room for maintenance work of the Information System (IS) equipment, infrastructure equipment and cleaning. An IT member should accompany such third parties and all the work should be done under their supervision. No third party is allowed inside the server room unless supervised by the C&IT department personnel.
4. If the proximity card database is not maintained then a Server room access register will be maintained which should provide details of the visitors who have visited the server room and the equipment accessed by them. In addition, the logbook should contain the details of the activity performed by visitors and is also countersigned by the accompanying IT department personnel.

Movement of assets in and out of the premises

Material going out

All movement of material in and out of premises should be controlled by security. All outgoing material needs to be accompanied by a gate-pass, which should be authorized by the Department/Division Head or above. The security personnel should check the material including IT assets against the gate pass and enter the details in a register. In case the IT asset is sent out for repairs, probable date of return should be noted. Manager–Administration should review the register on a weekly basis. In case return of asset is delayed by a week, the delay is pointed to the respective Department/Division Head and explanations are obtained from the vendor.

Material coming in

Security personnel should enquire about the nature of material, which is being brought in, and record the details in a register maintained to record the receipts. The concerned employee should be informed of the receipt of the material. The concerned employee should do an initial inspection and acknowledge the

receipt of the material. He/she should also sign in the register to acknowledge receipt of material. Manager-Administration will review the register on a weekly basis.

Physical security of assets

Desktops

The IT users assigned to every desktop are responsible for ensuring physical security of the desktops. All desktops should be backed up by UPS for protection against loss or fluctuation of power. The respective users should ensure desktop security against fire, water and dust. The users should lock their workstations before leaving it unattended; the workstations should be shut down before the user leaves the office. The users are also responsible include taking all possible steps to ensure safety and inform C&IT Department in case any event is noted.

Laptops

Due to the high risk of loss due to portability, laptops must be traceable to individual users, and sensitive data (to the extent possible) must not be stored on the unit's permanent disk drive.

All laptops must be physically secured via an appropriate security device during any period that the unit is left unattended. This may include laptop lock cable mechanisms and locking docking stations. Other secure and better devices may also be considered.

Networking equipment

The network Hubs/Switches/Routers located throughout the premise are placed in locked cabinets and should be protected from fire, heat, dust and water.

Network cable

Security Administrator (LAN & Network) would be responsible for power and telecommunications cables carrying data. The following controls should be considered:

1. Power and telecommunications lines into the premises and server room should be either underground or adequately protected.
2. Network cabling is protected from unauthorized interception or damage, by using conduits.
3. Power cables are segregated from communications cables to prevent interference.
4. Responsibility of the security of WAN components is of the Security Administrator (WAN) and supporting system executives.

Insurance

Insurance coverage must complement an effective system of physical security controls as a countermeasure against threat realization and impact on NMDC`s operations. The following items must be considered in regards to associated asset values versus insurance cost to mitigate losses:

a) IS equipment and facilities
b) Media reconstruction
c) Business interruption
d) Loss of items in transit

एन एम डी सी

NMDC

PHYSICAL ACCESS SECURITY POLICY

Insurance for loss of physical assets & consequential loss of business due to loss of data or non-availability of information systems: In case of consequential loss policy the premiums should be negotiated after showing the DRP & Backup procedures to the Insurance Company.