एन एम डी सी
NMDC

ACCESS CONTROL 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

ACCESS CONTROL POLICY

VERSION CONTROL

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

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

OBJECTIVE

The objective of this policy is to set guidelines for managing access to information and information processing facilities. In order to safeguard information and computing resources from various business and environmental threats, systems and procedures are developed and implemented for protecting them from unauthorized modification, disclosure or destruction to ensure that information remains accurate, confidential, and is available when required. The administration of user access to the company's automated information applies the principles of least privilege and "need to know" basis. Since NMDC is a leading PSU maintaining information confidentiality is critical. The procedures are administered to ensure that the appropriate level of access control is applied to protect the information in each application or system.

SCOPE

This document addresses policies and procedures related to the access control and rights on the information resources. This policy applies to all NMDC staff and all NMDC information resources including corporate data, as well as the application and systems software.

RESPONSIBILITY

System Administrator and the IT users are responsible for implementing and executing the procedures mentioned in this document. IT Security Nodal Officer will monitor the execution of the procedures.

Commented [BA1]: Roles to be defined

POLICY RULES

General principles

The access control policy shall always follow these general principles:

1. **Principle of least privilege**: A user account should be given only those privileges which are essential to that user's work. This helps reduce the "attack surface" of the computer by eliminating unnecessary privileges that can result in network exploits and computer compromises.
2. **Need-to-know:** This principle holds that access should be granted only to the information that one requires to perform one's task i.e. the person who has a legitimate business need for the information.
3. **Need-to-use:** This principle holds that access should be granted only to the information processing facility that one requires to perform one's task
4. **Segregation of duties (SoD):** It is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task. SoD involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control.
5. **Default deny:** Everything is generally forbidden unless explicitly permitted.
6. The access controls for an asset should always correspond to the associated information security risks.

User access management

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

The user access shall be managed to ensure authorized user access and to prevent unauthorized access to systems & services.

User registration and deregistration

A formal user registration and deregistration process should be implemented to enable assignment of access rights. Providing or revoking access to information or information processing facilities should be a two-step procedure – 1. Assigning, enabling or revoking a user ID and 2. Providing or revoking access rights to such user IDs.

1. **User identification**
   a) Unique user Identification:
   All users should be granted access to the computing resources through a unique user identification (user ID) at the operating system level (only if required, refer authentication policy domain) and the application level, the user ID will remain the same at both the levels.
   b) User ID naming convention:
   All user IDs will begin with initial letter of first name and will be followed by complete last name. In case such user id already exists, incremental digit will be added for each new user. Eg: asharma, asharma1, asharma2 etc.
   c) User credentials:
   User credentials consist of a user ID and password and/or other credential (such as digital certificates, token, etc.) that are unique to an individual. Personnel Department will maintain records for the user credentials with full name, job profile, relationship to the company and contact information.

2. **Creation of user ID**
   a) **Creation of new user IDs**
      New user IDs at operating systems, applications, and database and network levels shall be created based on formal authorizations on suitable requisition forms by the respective functional Head and the respective Security Administrator.
   b) **Use of common user ID**
      A common user ID is not to be used unless they are absolutely essential. Common user id for every department and one level of functional division under every department shall be created through the requisition form (Annexure 1). Common user IDs beyond these can be created only after specific written permission has been taken from system administrator, detailing the reason and users who have been granted the right to use this ID. These user IDs essentially should have a "read-only" access to the applications and an account with least privileges on the operating systems. E.g. As in the case of granting Common User IDs to any third party vendors working for NMDC and requiring access to its IT resources. But Common User IDs should be treated strictly as an exception and not as a practice and such IDs should be immediately removed after its purpose has been served.

3. **Control of user ID**
   a) Control over concurrent log on
      Users should not be allowed to log on simultaneously from more than one PC.
   b) Disabling inactive user IDs

User accounts that are inactive beyond a pre-defined period (Period to be decided by Asset administrator/30 days) should be disabled. The re-enabling of user accounts shall only be done on the request of the specific user.

c) Disabling or removing user IDs of separated employees

User accounts of employees who have left the organization on account of superannuation or resignation or termination or death, should be immediately disabled or removed.

d) Securing default user IDs

Default user IDs shipped with software and hardware should be disabled. Otherwise, the passwords should be changed in accordance with the NMDC's password policy.

e) User ID expiration dates for non-employees

For contract employees and consultants, an ID should only be created with an expiration date, coinciding with the conclusion of the contracted project. Security Nodal Officer IT should approve such creation.

f) System account suspension for failed login attempts

Three successive failures will result in a user's account being locked; they will not be able to login until their account is unlocked and the password reset. The user should contact the concerned Security Administrator for getting the account unlocked

g) Inactivity time out:

The terminals should be set to deactivate after ten minutes of inactivity. Additionally, password protected screen savers should be mandatory.

h) Desktop screen locking

All users should lock their terminals before leaving their workstations. Only the employee, whose session is active or the administrator should have an access to re login into the machine.

i) Clock synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which is required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs hinder such investigations and damage the credibility of such evidence. The Security Executive in charge of the network should ensure that users cannot change this setting.

j) System to notify user of last login/logout:

Upon login, the user is presented with date and time of last login and logout, along with contact information if they wish to report a discrepancy with their records.

k) Notifying security administrator of user job/function changes:

The supervisor of the user in question notifies Security Administrator of changes in the user's job function in order to ensure that access privileges are appropriately maintained.

l) Monitoring user activities

- All user activities will be logged by the operating systems and applications. The logs will be reviewed by the respective Security Executive on a daily basis. All unusual activities will be noted and investigated by them.
- New User IDs are specially monitored for a reasonable period to ensure that the access given is not used with malicious intent or that changes to data have not been made by mistake due to inexperience on the part of the user.
- Monitoring should also be done of users who are completing their notice period and have submitted their resignation letters.

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. The provisioning process for assigning or revoking access rights granted to user IDs should include:

1. Obtaining authorization from the owner of information system or service or management for the user of information system or service
2. Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties
3. Adapting access rights of users who have changed roles or departments and immediate removal of rights for users who have left the organization
4. Periodic review of access rights with owners of information system or service

Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled through a formal authorization process in accordance with the relevant access control policy. The following steps should be followed for implementation:

1. The privileged access rights associated with each system or process such as OS, database, application and users to whom they need to be allocated should be identified.
2. Privileged access rights shall be allocated on a need-to-use basis i.e. based on the minimum requirement for their functional role.
3. Regular activities should not be performed with privileged IDs.
4. If multiple administrators are present, then privileged access rights should be allotted to separate user IDs created specifically for the administrators. In exceptional cases where it can't be done, the confidentiality of secret authentication information shall be maintained.
5. Suitable system may be used for managing access to the servers wherever considered feasible and important.

Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process. The users should be informed about his responsibilities while using the system or service and must be compelled to keep the secret information confidential and never share it with any other user. The user should also be informed that the responsibility for misuse of account of such sharing shall lie solely with the user. A user policy may also be shared with the user through suitable means such as intranet, login screen etc.

Review of user access rights

Asset owners shall review users' access rights and privileged user access rights at regular intervals or after any changes.

Removal or adjustment of access rights

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change of role or transfer.

i. **Notification to systems engineers upon user termination/ transfer:**
   The Personnel Department immediately notifies the Security Executive upon the resignation, termination or transfer of employees
ii. **Revocation of user credentials:**
   The Security Administrators ensures that the user-ID is revoked upon termination or resignation of employees and revoked or access modified upon change of responsibilities (to be notified by functional head/RO1)
iii. **Separation of employees with access to sensitive information**
   For situations where users with access to highly sensitive information are separated, the employee's reporting officer is responsible for coordinating with the Administrators in charge to remove the user's access rights.
iv. **User clearance requirements**
   All PCs, keys, ID cards, software, data, documentation, manuals etc. of terminated or transferred employees are to be returned to the employee's reporting officer or the Personnel Department.
v. **Terminated employees**
   Depending on the nature of the termination, the employee may be subjected to varying levels of observation and escort considering the high possibility of mala fide intent.

User responsibilities

1. The users shall be accountable for safeguarding their authentication information;
2. Users shall be required to follow the user guidelines in the use of secret authentication information;
3. The users should be advised to change the authentication information on any indication of compromise and should inform the concerned administrator to check for indicators of such compromise;
4. The users should be advised to not use the same secret authentication information for business and non-business purposes;
5. The users may be required to choose quality passwords as per the NMDC password policy
6. All users should lock their terminals before leaving their workstations;
7. The user should inform of his change of responsibility to the concerned administrator.

Access to network & network services

Users shall only be provided with access to the network & network services that they have been specifically authorized to use. Following guidelines should be followed:

Segregation of networks

Data centre design for the organization network should be based on zone based security architecture containing three security zones: External, Internal and De-militarized Zone network with firewall. The applications and database servers should be setup in three separate zones (Internet Zone, ERP Zone and Intranet Zone for other application and services such as email, internet browsing, local company Intranet,

etc.) which shall be setup with appropriate security policies for each application access, so as to prevent the virus or worm attacks and can reduce the impact of attack.

Network security protection

The data centre should have the perimeter security firewalls deployed at both external and internal perimeters. Network Intrusion Prevention System (NIPS) shall be deployed in the external and internal access path of server zone and critical network segments, for analyzing traffic streams to identify and thwart network based attacks.

Endpoint security protection

Endpoint security protection shall be deployed on critical servers, applications and user desktops to protect against malware.

Authenticated & authorized access

Access to any network services shall be provided only after authentication of the user. Users shall only be provided with access to the services that they have been specifically authorized to use. User access for respective applications or servers shall be limited (as per authorization) to protect the applications, database, server setups from accidental or malicious damage.

Network connection control

Users should not connect any new resources onto data centre network without getting the prior approval from network administrator. All sensitive equipment and Servers should be designed/configured and implemented with appropriate means of physical and /or logical access. Network routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Physical and logical access to diagnostic and configuration ports shall be controlled.

Information, system and application access control

Segregation of responsibility

Each area of responsibility is clearly defined to avoid overlap in the functions performed by the Security Administrator/ Executive and also to assign accountability for each area. Additionally, if administration and monitoring functions are segregated for a specific component, the chances of fraud remaining undetected are reduced.

Security of system documentation

System documentation contains a range of sensitive information, for instance, descriptions of applications' processes, procedures, data structures, authorization processes. The following controls are considered to protect system documentation from unauthorized access:

a) System documentation is stored securely.
b) The access for system documentation is on a "Need to Know" basis and authorized by the respective administrator.

c) System documentation held on a public network, or supplied via a public network, is appropriately protected.

Publicly available information

Care is taken to protect the integrity of electronically published information to prevent unauthorized modification that could harm the reputation of the company. Information on a publicly available system, e.g. information on a Web server accessible via the internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place. The Security Nodal Officer- IT authorizes all changes before information is made publicly available.

Application and information access restriction

Access restrictions shall be implemented based on roles and privileges of the user. Access to information and application system functions should be restricted in accordance with the access control policy. Following may be used for access restriction:

d) Provide menus to control access to application system functions;
e) Control the access rights of users e.g. read, write, delete, execute;
f) Limiting the information contained in outputs
g) Provide protection from unauthorized access to any utility that is capable of overriding operating system (e.g. Shell Escapes in UNIX) or application controls
h) Do not compromise the security of other systems with which information resources are shared
i) Provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.

Isolation of sensitive systems

Sensitive systems (e.g. Fleet Management System, Financial Accounting System) require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity indicates that the application system is to run on a dedicated computer, only share resources with trusted applications systems. The following considerations apply:

a) The sensitivity of an application system is explicitly identified and documented by the Security Administrator.
b) When a sensitive application is to run in a shared environment, the application systems with which it shares resources are identified and agreed with the Security Administrator in charge of the sensitive application.
c) The Security Administrator ensures that critical events, like the failed logons, are adequately logged and that these logs are reviewed on a regular basis.

Secure-log-on procedures

Access to systems and applications containing sensitive information shall be controlled by secure log-on procedures. The log-on procedures should:

a) Not display system or application identifiers until the log-on process has successfully completed;

b) Display a general waring banner immediately on domain logon that warns the user that the application or service or system shall only be used by authorized users and that by logging on to NMDC domain they agree to comply with the company's IT rules and regulations:
"*** Warning ****
This computer system is the property of the NMDC. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, the NMDC Use of Information Technology Resources Policy. Unauthorized or improper use of this system may result in disciplinary action as per the NMDC conduct rules."
c) Not provide help messages during log-on procedure that would aid an unauthorized user
d) Log successful and unsuccessful attempts
e) Not display a password being entered
f) Not transmit passwords in clear-text over public network
g) Restrict connection times to provide additional security for high-risk applications
h) Terminate inactive sessions after a defined period of inactivity

Password management system

Password management systems shall be interactive and shall ensure quality passwords in accordance with NMDC's password policy. A password management system should:

a) Enforce password complexity commensurate with business risks associated with data
b) Allow users to select and change their own passwords unless assigned by independent authority
c) Force users to change their passwords on first log-on unless assigned by independent authority
d) Not display the passwords on the screen while being entered
e) Store password files separately from application system data
f) Enforce password aging in systems and processes dealing with sensitive data

Use of privileged utility program

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

Access control to program source code

Access to program source code and associated items shall be restricted, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. Preferably source codes may be stored in program source libraries. Following guidelines may be used to control access to such libraries to reduce the potential for corruption of programs:

a) Where possible, program source libraries should not be held in operational systems
b) Systems Executives responsible for the application will approve accesses to the program source library of the application;
c) Support personnel should not have unrestricted access to these libraries;
d) Updating of these libraries should be performed only after obtaining proper authorization;
e) Program listings should be held in a secure environment;
f) An audit log is maintained of all accesses to program source libraries;

g) Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures;
h) Maintenance and copying of program source libraries should be subject to strict change control procedures

Responsibility:

Security Administrator- Business Applications Group is responsible for monitoring the information asset access controls.

It is the responsibility of IT users and/or reporting officers of the users at each unit to formally intimate the Security Administrator about any change in their roles and responsibilities, which affect the access controls.

Access rights to 'Third Parties'

Access given to third parties for the NMDC's information resources should be restricted and governed by the same general principles enunciated above. Following guidelines may be followed for such grant of access rights to third parties:

a) The company's employees coordinating with the respective third party consultants, engineers, vendor's representatives etc. are responsible for justifying and authorizing the access rights granted to third parties.
b) The third party representatives will be primarily restricted to use company's information resources from within the company's network. However, if under any circumstances remote access to the network has to be given to third parties then it should be either a dedicated channel of communication or a secured VPN tunnel.
c) Access rights to consultants and software developers ('third party') such as Vendor Helpdesks and implementation teams are formally granted and monitored. The relevant rights are revoked once the required assignment is over. The third party is primarily restricted access to 'View Only' of the live environment.

Following are the procedures that should be followed while granting the access rights to the third party:

a) An access rights form should be completed by the third party and approved by the employee who is dealing with the vendor. Thereafter it has to be approved by the concerned system/process administrator and functional head as per the sensitivity of the information processing facility to be accessed.
b) In case the third party wants to modify any data they need to obtain approval from the respective department head and communicate the approval to the concerned Security Administrator.
c) On receiving intimation from department head and data owner, the system administrator should create a user ID for the third party.
d) The password for the said ID should be communicated in accordance with the NMDC's Authentication policy
e) The system Administrator should periodically review the activity logs generated to monitor activities performed by the third party.

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

Remote access to NMDC network

Remote access will be disabled by default and allowed on a case to case basis.

Remote access to NMDC network for using any system or service/application in data center from public network should be handled with special care since it introduces a vulnerability to the Information processing infrastructure as a whole. Following guidelines may be followed:

a) Two-factor authentication shall be used for such access.
b) Separate authentication servers may be established in tandem with perimeter firewalls to authorize such users.
c) General user creation and access rights provisioning may be followed by system administrator and VPN administrator with special care to get prior authorization from appropriate authorities.
d) Proper access roles may be identified and appropriate controls should be enabled to limit accessibility to these resources.

All dial-up access to NMDC networks and computer systems must be protected by a strong security layer separate from the system security layer that will authenticate users and permit them to access only those networks, computer system, and applications for which they have been properly authorized.

Approval and Registration of Dial-Up/Remote Access

All new procurements or service requests which have components or services related to dial-in or remote access must be reviewed and approved through the requester's respective management and security officer for approval and tracking.

The review and approval process must evaluate:

a) Appropriateness of the requested dial-up/remote access application
b) Selection of appropriate dial-up access entry points
c) Documentation of the requested equipment
d) Tracking of the respective service, software, or equipment.

Dial-Up Access to Local Area Networks

Local area networks and other multi-user departmental systems must utilize a limited number of centralized communication servers or equivalent modem pooling configurations for all dialup access applications.

Dial-Up Access to Workstations

While connected to network computing resources, modems on computers must not be enabled in auto answer mode (permitting in-bound access). Installation of telecommunications components required for dial-up or remote access must be configured to restrict access to the necessary business needs.

Dial-Up Access to Diagnostic/Maintenance Ports

All dial-up access connections for equipment diagnostic and maintenance purposes (e.g., frontend communications processor support and network router programming/diagnostics), must be designed and implemented in a manner that ensures compliance with this standard.

Commented [BA2]: Not in use – Department may choose to remove this section

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

Remote Control Access

Only NMDC approved remote control configuration and software should be used for remote control access to information systems. Insecure utilities such as telnet should not be used for remotely accessing the servers. All processors being controlled remotely must be physically secured in a manner which prevents tampering while in use or awaiting use.

Authentication Methods

Dial-up access controls must be implemented only through a strong two factor authentication which should be approved solution and may meet all of the following requirements:

a) Unique identification or access code (user ID) for each user
b) Capability to restrict users to only those networks, computer systems, and applications for which they have been properly authorized
c) Access control software/hardware that protects stored data and the security system from tampering
d) Audit trails of successful and unsuccessful log-on attempts
e) Automatic system reboot or session cleanup following the disconnection of incoming dial-up sessions
f) Capability to limit the number of unsuccessful log-on access attempts
g) Appropriate verification of the dial-up user's identity by approved methods of authentication, consistent with the sensitivity and technical attributes of the dial-up application

Exception Criteria

Requested exceptions to the standard must be submitted to the Security Officer (SO). Exceptions will be reviewed by the SO, who may request that a risk analysis be performed to determine what security measures are appropriate. Exceptions may be granted after the SO determines that an appropriate compensating control exists. Exceptions will be reviewed as short term resolutions.

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

ANNEXURE

Annexure 1: Requisition for creation of new account on server

Unit :	Date:
Name of the user:	Department :
Server Name:	
Operating system:	
Application systems & Data files :	
Other OS privileges: (e.g. FTP, remote login etc.)	
Requisitioned by:	
Reason for requisition:	
Authorization: Grant the following access rights to the user:	
Revoke the following rights/ privileges to the user:	
For third parties/temporary hires/contractual workers Access start date: _/_/_ Access end date: _/_/_	
Authorized by : Date:	
For Office Use only:	
Access granted to the user:	
Access revoked for the user:	
User id created:	Systems Group allotted:
Performed by: Date:	

Annexure 2: Requisition for access rights of application systems

Unit:	Date:
Name of the user:	Department:
Application System:	
Menu options:	
Database access rights:	
Requisitioned by:	
Authorization: Grant/ modify the following access rights to the user.	
Revoke the following rights to the user	
Authorized by :	Date:
For Official Use only: Access granted to the user:	
Access revoked for the user:	
User ID created:	Systems Group allotted:
Performed by:	Date

एन एम डी सी
NMDC

ACCESS CONTROL POLICY

Annexure 3: Notification to security administrator for change in user job function

Unit name:	Date:
To:	From:
Kindly note the change in the job function of Mr./Ms._____with effect from _/_/_ as follows:	
Old Job Specifications:	New Job specifications:
Old systems rights:	New system rights:
Please refer to the access rights form attached herewith.	
Approval of Security Administrator and Remarks: Date:	
For Official Use Only: Access granted to the user:	
Access revoked for the user:	
User ID created:	Systems Group allotted:
Performed by: Date:	

Annexure 4: Notification to security executive for termination/transfer/ resignation of user

User:	
Unit name	Date:
To	From:
Kindly note that:	
1. Mr./Ms. _____has been transferred with effect from _/_/_ to _____unit	
2. Services of Mr./Ms. _____have been terminated with effect from _/_/_	
3. Mr./Ms. _____ has resigned from service with effect from _/_/_	
Approval of Security Administrator and Remarks: Date:	
For Official Use Only: Access revoked for the user:	
User ID revoked:	
Performed by: Date:	