एन एम डी सी
NMDC

# AUTHENTICATION 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

# AUTHENTICATION POLICY

**VERSION CONTROL**

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

एन एम डी सी
NMDC

# AUTHENTICATION POLICY

## OBJECTIVE

The purpose of this policy is to establish a standard for authentication of users to the IT systems and creation of strong passwords, the protection of those passwords, and the frequency of change. In order to safeguard information and computing resources from various business and environmental threats, systems and procedures are developed and implemented for authenticating users so that only authorized users are given access to the organizations' computing resources. Strong authentication (two factor) shall be used for all critical applications & databases.

NMDC has business data spread across multiple servers and location. These servers' process and data are worth millions of rupees hence authentication of users has to be strictly controlled as per the procedure mentioned hereunder.

## SCOPE

This document addresses Policies and Procedures related to the authentication of users to the organization's information resources. This Policy applies to all NMDC staff and all NMDC information resources including all operating systems, applications, databases, LDAP and all other computing resources.

## RESPONSIBILITY

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

## POLICY RULES

### User Authentication

**Hardware Layer**

All desktops and servers should have Power On password enabled on them to avoid unauthorized access to the IT resources. These passwords should also comply with the passwords management procedures mentioned in the Password Management section hereunder.

**Commented [BA1]:** Department to confirm if power on password is to be implemented

**Application Layer**

To access business applications like FAS, HRMS etc. all users necessarily have to authenticate themselves to the application or the database.

**Operating System Layer**

To access the network resources like file server, print server, proxy server etc. users must necessarily authenticate themselves to the operating systems. The domain controller will contain a directory dedicated for each user. The directory should be used to store all the data by the users instead of their local machines.

**Commented [BA2]:** Department to confirm

User IDs on the servers running business applications should be created only at the application level and not at the Operating System level. The user should not be able to access the command prompt.

एन एम डी सी
NMDC

# AUTHENTICATION POLICY

To create users at the operating system level, authorization has to be taken from the respective Security Administrator and the Security Officer.

## Password Management

**Confidentiality of Passwords**

1. User passwords should remain confidential and not shared, posted or otherwise divulged in any manner.
2. Users should sign confidentiality agreement at the time of joining the organization; Personnel department will be responsible for implementing this.
3. Auto-saving of passwords shall be disabled.

**Password Composition**

Commented [BA3]: Department to confirm if such composition can be implemented

1. Passwords should consist of at least six characters.
2. The passwords selected should contain at least 2 uppercase, 1 lowercase, 1 numeric and 1 special character.
3. The passwords should not contain the user name, user id/login id, spouse/child's name, nmdc or a combination of them.
4. Password should be different at the operating system and the application level.
5. Password should not contain simple combinations like abcd, 1234, etc.
6. Password should not contain months of the year, days of the week or any other aspect of the date

**Password Expiration**

1. Passwords should expire after a maximum period of 60 calendar days.
2. A given password should not be used more than once in 180 calendar days. Alternatively, the same password should not be repeated within a cycle of 3 password changes.
3. User will be prompted to change password every day starting 5 days before expiry of password.

**One Time Use of Initial Passwords**

1. The Systems Administrators should provide users with an initial password and configure the system to force the users to change the passwords immediately after the first logon.
2. Users should be provided with the capability to change their password on the login interface (after authentication).

**Password Reset**

Via portal

**Password Backups**

1. All password backups for critical user-IDs should be kept with IT Security Nodal Officer.
2. The Security Administrator should identify the critical user-IDs and their passwords and maintain record of their passwords. This is necessary in case the related person has left the organization without surrendering the passwords.

**Power-on Password**

एन एम डी सी
NMDC

# AUTHENTICATION POLICY

1. Users should be encouraged to use the power-on passwords (for critical workstations, laptops and thin clients).
2. Sharing of power-on passwords to be allowed only if multiple users need to access the same system physically and the passwords should be maintained solely within the members of the group sharing the system.
3. The power-on passwords should be subject to the same controls as personal passwords.

**Account Lockout**

1. Three successive failures must result in a user's account being locked out.
2. The users will not be able to login until the account is unlocked and the password reset. The user should submit a formal request to the Systems Administrator to carry out the exercise.

**Other Miscellaneous Best Practices**

1. Disabling Default Passwords: Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems should be promptly changed. Default passwords shipped with software should be disabled or changed.
2. Prohibition of Group Passwords: Group passwords should not be allowed to the extent possible so that individual accountability is maintained. Where used, they should be maintained solely within the members of the group, and should be subject to the same controls as personal passwords.