एन एम डी सी
NMDC

ENCRYPTION 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

ENCRYPTION POLICY

VERSION CONTROL

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

एन एम डी सी
NMDC

ENCRYPTION POLICY

OBJECTIVE

NMDC shall provide maximum protection to classified, sensitive and confidential information identified by the company by efficiently utilizing data encryption. The need and the extent of utilization of data encryption methods shall be justified by clear business objectives, nature of technology, information classification and the resultant risk to the information resources.

Further, NMDC shall implement suitable encryption measures for any data being sent over third party networks and communication backbone. While implementing these encryption methods NMDC shall adopt best standards for encryption and effective key management practices.

The objective of this policy is to set a guideline for usage of encryption methods and management of the encryption software for maintaining integrity and confidentiality of protect information that contain, process, or transmit confidential and firm-sensitive information

SCOPE

This policy applies to all employees of NMDC and all entities that use NMDC's computing and networking resources. This includes contractors, consultants, third party associates and any temporary employees. It covers all systems, information, and facilities used to create/manage/use the process of exchanging and storing encrypted data among NMDC components and transactions involving outside agents. It is applicable to all data, information, knowledge including e-mail and web server.

RESPONSIBILITY

The Security Officer-IT Communications is the executive owner of this document. However, the responsibility of implementing and executing the procedures mentioned in this document lies with the Mail administrator, Web administrator and Systems Administrator of the IT Team. The execution of the procedures will be monitored by Security Manager.

POLICY RULES

General principles

1. Information used to verify the identification and other parameters that can be used to gain access to services, on corporate systems must be appropriately protected.
2. Static or reusable authentication information must be encrypted during storage and while passing through the network using encryption software or hardware.
3. NMDC uses <describe encryption used e.g. AES, 3DES, RSA> technology (ies) for encrypting confidential and other firm sensitive data, unless documented through the exception process as described below. Symmetric cryptosystem key lengths should be at least 80 bits for confidential data and 64 bits for other sensitive information identified by the firm. Asymmetric crypto-system keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit =1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit). All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to AES 128-bit encryption.

Commented [BA1]: What all data are being encrypted currently (and what is the technology used? Check if file folders, shared files are encrypted) –department to confirm

एन एम डी सी
NMDC

ENCRYPTION POLICY

4. The strength of the encryption algorithm to be used in a given situation must be based on the classification of the data to be encrypted. This shall apply for any B2B or B2C communication between NMDC and any other party. For e.g. any financial transaction over the Internet, in the scenario of a transaction web site hosted by NMDC must be 128-bit SSL.
5. The use of proprietary encryption algorithms are not allowed for any purpose.
6. NMDC's key length requirements will be reviewed annually and upgraded as technology allows.

Use of encryption

Encryption technology must not be used for confidential/restricted company information unless the technology has first been approved by the company's management.

Access to encryption software

1. Access to encryption software must be restricted to authorized personnel only.
2. All encryption activities (generation of keys, loading, storage etc.) should take place within a secured facility

Review of encryption procedures

The encryption algorithm and standards used must be reviewed every year to ensure that these are updated with latest standards and regulatory requirements.

Data encryption

Commented [BA2]: Data at rest and data transmitted are not encrypted currently
Department to decide on feasibility

Data at rest

1. To prevent unauthorized disclosure of data when computers are sent out for repair or used by personnel, other than the regular users within or outside the organization, all data stored on hard disks must be encrypted.
2. Hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.
3. Confidential data at rest on computer systems owned by and located within controlled spaces and networks are protected by
   a) Encryption with strict access controls that authenticate the identity of those individuals who access the specific system or data
   b) Other compensating controls including complex passwords, physical isolation, etc.
4. NMDC secures its back up and stored data on file systems, disks, heterogeneous tape drives, virtual tape libraries in a Storage Area Network/ Direct-Attached Storage/ Network Attached Storage environment.
5. Firm sensitive back up data is protected using AES 256-bit algorithm or identical live data encryption methodologies.
6. In case of a hard disk damage /any media crash, it should be ensured that repair is done on NMDC premises and in case of replacement, the original hard disk is returned to the possession of NMDC.

Commented [BA3]: To include in AMC contracts

एन एम डी सी
NMDC

ENCRYPTION POLICY

7. Disk Drive Degaussers should be used to sanitize (degauss) all Computer hard drives or other storage media that have been encrypted (i.e. Tape drives, Hard Disk Drives etc.) to prevent unauthorized exposure.

Commented [BA4]: Department to discuss with AMC provider

Commented [BA5]: To be implemented through MDM

Mobile devices

1. Mobile devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential data are the result of stolen or lost mobile computing devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. As a general practice, confidential data should not to be copied to or stored on a portable computing device. However, in situations that require confidential data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.
2. Confidential information stored on mobile devices must be encrypted using products and/or methods approved by the Security Officer [such as full disk encryption with pre-boot authentication].
3. Mobile devices including, laptops, tablets, smartphones etc. should not be used for the long-term storage of any confidential information.
4. Portable laptops containing sensitive data (non-disclosure) must be protected using a PC Security/Disk Encryption Package
5. Mobile devices that store or transmit confidential information must have the proper protection mechanisms installed, including password protection, antivirus/firewall software, and subject to needed applications being properly configured.
6. Confidential information not being actively used, when stored or transported in computer readable storage media (such as servers, magnetic tapes, floppy disks or CDs, DVDs, USB memory drives etc.), must be in an encrypted form. The media should be stored in a secure (preferably locked) location.
7. Removable media that contain confidential information must be transported using a secure manner <to ensure tamper proofing while packaging>.
8. Media that is sent offsite for storage by third party must have accompanying chain of custody forms for possession tracking of media.
9. Mobile or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g. must not be checked as luggage while in transit). The receiver of the removable media must be identified to ensure the person requesting the data is the one claimed. Data security rests with the authorized user.
10. NMDC will inventory encrypted devices and validate implementation of encryption products at least annually.
11. Data owners and users of mobile devices containing confidential data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:
    a) Maintaining an accessible copy of the data on a server managed by the firm, using procedures specified by the Security Officer.
    b) Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
    c) Escrowing the encryption key with a trusted party designated by the data owner and the Security Officer.

एन एम डी सी
NMDC

ENCRYPTION POLICY

Data transmission

1. Users will follow acceptable use policies when transmitting data and must take particular care when transmitting or re-transmitting confidential data (e.g., citizen personal identification information) received from non-firm employees.
2. Confidential information transmitted as an email message must be encrypted. In mail server, separate encryption keys should be created for users who frequently communicate and transfer confidential information with external entities for business purposes via e-mail. Further, confidential documents can be encrypted using a public and private key combination. These keys can be added to the form for creating such documents.
3. Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with must be encrypted or be transmitted through an encrypted tunnel that is encrypted with virtual private networks (VPN) or point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).
4. Transmitting unencrypted confidential information through the use of web email programs (Yahoo, Gmail, etc.) is not allowed.
5. The download or installation of any Instant Messaging (IM) or online peer-to-peer (P2P) file sharing programs requires specific authorization in writing from the Security Officer or designated official. All approved P2P or IM networks will use tools that encrypt the traffic flows between peers and only allow access to a managed IM server which provides gateways to public services.
6. Wireless (Wi-Fi) transmissions that are used to access NMDC's mobile devices or internal networks must be encrypted using IEEE 802.11i (WPA2) or better, and any VPN exceptions for remote wireless and/or internal network configurations standard.
7. Encryption is required when users access NMDC data remotely from a shared network, including connections from a Bluetooth device to a mobile device.
8. Confidential/restricted information transmitted over any shared or third party communication network including back up, PSTN lines etc. must be sent in an encrypted form.
9. NMDC generally blocks FTP. It is enabled through Firewall only and using secure file transfer programs <such as "secured FTP" (FTP over SSH) and SCP>.
10. To use the transmitting server securely, each authorized user must have a logon ID and password with a designated directory.
11. Users should not have access to shared directories unless required for business reasons.
12. Anonymous FTP is not permitted.
13. All accounts and keys must be managed from within NMDC network.
14. All transactions and transfers must be logged, and reviewed for prohibited activity.
15. All files contained within an account's directory must be deleted seven days after they are delivered or made available for retrieval.
16. Plain FTP does not provide encrypted transmission and should not be used on any Internet-facing systems or where confidential data is being transmitted.

Key Escrow

Commented [BA6]: Department to check and confirm

Commented [BA7]: Department to check and confirm

एन एम डी सी
NMDC

ENCRYPTION POLICY

1. Escrow functions must be available with the encryption system to enable decryption and recovery of data in the event of inability to decrypt due to system errors, human errors, or any other problems.
2. Knowledge and access of the escrow function must be restricted to authorized persons.

Digital Signature

1. Keys used for digital signatures, digital certificates, and user authentication must never be included in a key escrow management to eliminate any impersonation, which in turn facilitates fraud and deceit.
2. The company shall ensure that the vendor of digital signature applications have required permissions of export before adopting any standardized application.

Other Applications

Any data including video or audio to be sent using public network would be done only using secure encrypted channels like VPN etc. This would be applicable for any application doing video conferencing, chat etc.

Commented [BA8]: Department to check with Railtel

Encryption key management

Commented [BA9]: Department to check current encryption key management processes

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

Process of generating encryption keys

1. Encryption keys must be generated by means, which will yield keys that are difficult to compromise.
2. Whenever user-chosen encryption keys are employed, the encryption system enforce users to employ keys of the designated strength, as decided by the Security Officer.
3. The company's encryption documentation should use a standard naming conventions (e.g. ANSI X.9) for the keys so as to facilitate communication while dealing with multiple hardware, platforms, software vendors and outside parties.
4. It should also be ensured that each key has a single purpose (e.g. either storage keys or transporting key)
5. Keys must be randomly chosen from the entire key space, using hardware-based randomization.
6. Key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.
7.

Life (Maximum) of encryption Keys

Encryption keys must be changed every ninety days in case of a fully functional deployment of a Public Key Infrastructure at an Enterprise level or for commercial certifications.

NMDC uses short key life or crypto periods with defined activation and deactivation duration limits; for the following key types with maximum crypto periods for originators and Recipients as indicated below. Originator Usage Periods (OUP) are differentiated from Recipient Usage Periods when applicable < e.g., Symmetric Authentication Key: 2 years, OUP + 3 years; Private or Public Authentication Keys: 1-2 years.>

एन एम डी सी
NMDC

ENCRYPTION POLICY

Keys with a longer life are sparsely used and must be approved by the Security Officer. The key shall be destroyed at the end of its crypto period. (The cost of changing keys rises linearly while the cost of attacking the keys rises exponentially. Therefore, all other factors being equal, changing keys will increase the effective key length of an algorithm.)

Life (Minimum) of readable data after encryption

The source version of the data that has been encrypted must not be deleted unless it has been demonstrated that the decryption process can re-establish a readable version of the data.

Disclosure of encryption keys

1. Encryption keys are the most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know.
2. Unless the approval of the company's Security Manager/Security Officer is obtained, encryption keys must not be revealed to consultants, contractors, or other third parties.

Protection of Encryption Keys

1. Key management should be fully automated, NMDC personnel should not have the opportunity to expose a key or influence the key creation.
2. Where possible encryption keys must not be transmitted over the network.
3. Keys in storage and transit must be encrypted.
4. Private keys must be kept confidential.
5. Keys that are transmitted are sent securely to well-authenticated parties.
6. The company's encryption systems must be designed such that no single person has full knowledge of any single encryption key which is critical. This must be achieved by separation of duties in such a way that two people must be present for an important activity or by "Key Splitting".
7. Key management responsibility may only be delegated to a party who has passed a background check, operational security audit and signed a confidentiality agreement, if NMDC implements an Enterprise wide Certification Authority or goes for a Commercial Certification Authority to implement Public Key Infrastructure.
8. NMDC uses procedural controls to enforce the concepts of least privilege and separation of duties for personnel. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor personnel.
9. The Security Officer will verify backup storage for Key passwords, Files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.
10. To ensure separation of duties and two person control, <Secondary Director/Manager> is responsible for encryption key management functions.
11. No single individual is authorized to generate a new CA key pair.
12. Quarterly audit reviews are conducted.
13. Key management personnel must complete annual training on key management requirements and procedures.
14. Job rotation will take place biennially among key management personnel.
15. While storing encrypted data, the encryption keys and other encryption material used to encrypt,
    a) Must not be stored on the same media as the encrypted data

b) Must be stored in an encrypted form

16. The encryption keys must be encrypted with a stronger algorithm than what is used for encrypting the data.
17. Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure.
18. Protection of Master keys
    a) Master keys must always be stored in encrypted form.
    b) Master key must be handled with dual responsibility with split knowledge.
    c) Master keys must be stored in tamper-proof modules.
    d) Master keys must not be transmitted over the network.
19. The NMDC key management system or vendor will provide written security policies and procedures that address encryption key:
    a) Generation processes for different cryptographic systems and different applications
    b) Distribution, access, and activation for authorized users
    c) Storage, Archiving, and Destruction
    d) Changes and updates, including rules on when keys should be changed and how this will be done;
    e) Compromises or loss of control incidents
    f) Revocation with specific withdrawal or deactivation procedures
    g) Audit logging of management-related activities
    h) Activation and deactivation dates and usage period limits
    i) Recovery when lost or corrupted as part of business continuity planning
    j) Roles, responsibilities, facilities, and procedures for all organizational elements to reliably recover critical data <e.g., storing an escrowed recovery key on a USB device and/or protecting with a numeric password>.
    k) Specification of circumstances and process for authorizing key recovery.
    l) Generation (e.g., whether or not the material was centrally-generated),
    m) Storage and access for long-term storage keys.
    n) Process of transitioning from the current to future long-term storage keys.

Management of keying material

1. All materials used for generation, distribution and storage of keys must be destroyed by pulping, shredding, burning or other approved methods to prevent from any unauthorized disclosure.
2. Custodians of keying material must destroy this material according to approved procedures within one business day following the successful verification of a key exchange process.
3. The company must maintain an updated inventory of all keys, components of keys and cryptographic hardware. This list should be referenced any time manual intervention takes place to ensure that the key or device is legitimate.
4. The encryption keys should never be shared between more than two parties. A key should never be included in a key sharing transaction with a third party, even if they are trusted partner. This reduces the number of parties that must be contacted in the event of a key compromise and prevents the third party from accessing confidential data or the keys necessary to decrypt that data.

एन एम डी सी
NMDC

ENCRYPTION POLICY

Exception Process

Under certain circumstances the Security Officer may grant or issue an exception to the use of encryption on mobile devices containing confidential NMDC data.

Exceptions are of two types: 1) an exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type should be in writing and should be initiated by the data owner. 2) Broader exceptions may be issued to cover circumstances that span NMDC as a whole. Requests for exceptions of this type may come from any person, or such exceptions may be initiated by the Security Officer.

The Security Officer must approve and document all exceptions based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure and the potential adverse consequences for individuals, other organizations, or NMDC if an exposure occurs as a result of the exception.

As a condition for granting an exception, the Security Officer of NMDC may require implementation of compensating controls to offset the risk created by the lack of encryption.

Exceptions must be documented and must include the following elements:

a) A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included
b) The rationale for granting the exception
c) An expiration date for the exception
d) A description of any compensating security measures that are to be required.

Disciplinary Actions

Violation of this policy, [e.g., willful or negligent exposure of confidential information,] may result in disciplinary action which may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with NMDC. Additionally, employees, contractors and agents who violate this policy may be subject to civil and criminal prosecution under the law.

Commented [BA10]: Department to confirm if such disciplinary actions can be taken for policy violations as per NMDC code of conduct