# Encryption

Table Of Contents

## 1.1 Policy Statement

Kshema must ensure that the restricted/ confidential data must always be in an encrypted form while in transit and when stored on a storage media. Further, any information traveling over third party networks must also be encrypted. Encryption must be achieved by adopting best standards for encryption and effective key management practices.

## 1.2 Scope

This Policy Statement applies to all information users of Kshema, and all personnel who use and have access to the Kshema's computing and networking resources. This includes, contractors, consultants, third party associates and any temporary employees. It covers all systems, information technology, and facilities used to create/manage/use the process of exchanging encrypted data among Project components and transactions involving outside agents. It is applicable to all data, information, knowledge including e-mail and web server.

## 1.3 Execution Responsibility

The CISO along with Administrator-Network & Administrator-Systems is primarily responsible for implementing the procedures mentioned in this chapter on encryption. The overall monitoring and execution responsibility lies with the Head-Infrastructure. The Internal Auditor performs periodical checks to ensure compliance with encryption standards.

## 1.4 Detailed Procedures

### *14.2.1 Data Encryption*

#### *14.2.1.1 Data over third party networks*

Any data travelling over third-party networks must be encrypted using appropriate technology.

#### *14.2.1.2 Encryption of confidential / restricted information*

Confidential / restricted information transmitted over any communication network, must be sent in an encrypted form.

Confidential information not being actively used, when stored or transported in computer-readable storage media (such as servers, magnetic tapes, floppy disks or CDs), must be in encrypted form.

Information used to verify the identification of users or other objects such as credit card numbers, telephone calling card numbers and other parameters that can be used to gain access to goods and services, on corporate systems must be appropriately protected. Static or reusable authentication information must be encrypted during storage and while passing through the network using encryption software or hardware.

To prevent unauthorised disclosure of data when computers are sent out for repair or used by others within or outside the organisation, all data stored on hard disks must be encrypted via user-transparent processes.

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.

#### *14.2.1.3 Use of Encryption*

Encryption technology must not be used for encrypting sensitive data unless the technology has first been approved by CTO.

#### *14.2.1.4 Access to Encryption Software*

- Access to encryption software must be restricted to authorised personnel only.
- All encryption activities (generation of keys, loading, storage etc.) should take place within a secured facility as defined in the chapter "Physical Security".

#### *14.2.1.5 Review of Encryption Standards*

The encryption algorithm and standards used must be reviewed every year to ensure that these are updated with latest standards and regulatory requirements. This may include compliance with the local laws and regulatory requirements in terms of encryption strength, algorithms etc.

### ***14.2.2 Encryption Key Management***

#### *14.2.2.1 Process of Generating Encryption Keys*

- Encryption keys must be generated by means, which will yield keys that are difficult to compromise.
- Whenever user-chosen encryption keys are employed, the encryption system must prevent users from employing keys made up of less than twelve characters.
- The Kshema's encryption documentation should use standard naming conventions (e.g. ANSI X.9) for the keys so as to facilitate communication while dealing with multiple hardware, platforms, customers and third parties.
- It should also be ensured that each key has a single purpose (e.g. either storage keys or transporting key)

#### *14.2.2.2 Life (Maximum) of Encryption Keys*

Encryption keys must be changed every ninety days

#### *14.2.2.3 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.

#### *14.2.2.4 Disclosure of Encryption Keys*

- 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.
- Unless the approval of the MISF is obtained, encryption keys must not be revealed to consultants, contractors, or other third parties.

#### *14.2.2.5 Protection of Encryption Keys*

- Where possible encryption keys must not be transmitted over the network. If the keys used to govern the encryption process are to be transmitted over the network then they must be transmitted through separate communication channels such as Telephone.
- The Kshema's encryption systems must be designed such that no single person has full knowledge of any single encryption key. This must be achieved by separation of duties in such a way that two people must be present for an important activity by "Key Splitting".
- Key management responsibility may only be delegated to a party who has passed a background check, operational security audit and signed a confidentiality agreement.
- While storing encrypted data, the encryption keys and other encryption material used to encrypt,
  - Must not be stored on the same media as the encrypted data
  - Must be stored in an encrypted form
- The encryption keys must be encrypted with a stronger algorithm than what is used for encrypting the data.

#### *14.2.2.6 Protection of Master keys*

Master Keys must always be stored in encrypted form, except in the following approaches.

- Master Key must be handled with dual responsibility with split knowledge.
- Master Keys must be stored in tamper-proof modules.
- Master Keys must not be transmitted over the network.

#### *14.2.2.7 Management of keying material*

- 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 unauthorised disclosure.
- 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.
- The Kshema 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.
- 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 both 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.

### *14.2.3 Key Escrow*

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. Knowledge and access of the escrow function must be restricted to authorized persons.

### *14.2.4 Digital Signature*

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. The Kshema must ensure that the vendor of digital signature applications have required permissions of export before adopting any standardized application.

### *14.2.5 Related Information on Encryption Standards*

The following are some of the key encryption standards/regulations widely used across the industry. The Kshema should, where possible, comply with these.

### *14.2.6 Restrictions on Export of Encryption Technology*

The encryption software or any technical data associated with it, must comply with international standards governing their distribution or export (e.g. US International Trade in Armaments Regulations, US Govt. Federal Regulations and Bureau of Export Administration of the Department of Commerce).

### *14.2.7 Standard Encryption Algorithm & Implementation*

Without any standard International conventions, it may be appropriate to choose any algorithm that has a wider acceptance. Here is a list of Standards that are widely accepted in different countries by their local governments (e.g. ANSI X9.9, ANSI X.9.23, ANSI X.9.28, ANSI X9.17, ITU-T (CCITT) X.509, ISO/IEC 9798 and IEEE P1363)

### *14.2.8 Public Key Cryptography Standards (PKCS)*

In the event of Public Key Encryption, RSA is the most widely used public key crypto system at present. Public Key Cryptography Standards are widely used set of standards for public key cryptography, developed under the leadership of RSA (Rivest Shamir Adleman) Data Security.