* **Cryptography policy**

**Cryptography**- It is a technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it.

**Features of Cryptography are as follows:**

1. *Confidentiality: Information* can only be accessed by the person for whom it is intended and no other person except him can access it.
2. *Integrity: Information* cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. *Non-repudiation*: The creator/sender of information cannot deny his or her intention to send information at later stage.
4. *Authentication:* The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

***There are two types of Cryptography in general. They are-***

1. **Symmetric Key Cryptography:**

* It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.
* Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner.
* The most popular symmetric key cryptography system is Data Encryption System (DES).

1. **Asymmetric Key Cryptography:**

* Under this system a pair of keys is used to encrypt and decrypt information.
* A public key is used for encryption and a private key is used for decryption.
* Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

*This policy defines the controls and related procedures for the various areas where encryption and other cryptographic techniques are used-*

* All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.
* The Data Handling Procedures require that the storage of sensitive data in some locations be encrypted.
* The Data Handling Procedures require the transfer of sensitive data through a secure channel. A secure channel is an encrypted network connection.
* Various methods of encryption are available and generally built-in to the application. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.
* Access to sensitive data via a website, web application or mobile app. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices
* The Data Handling Procedures require that when emailing some sensitive data, the message and attachments be encrypted.