

**CRYPTOGRAPHY CONTROL POLICY**

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 1.0 | 29th July 2015 | Baseline & Release | Rahul Raj | Dhananjay | Ajay Kumar Zalpuri |

# 1. Cryptographic controls

Mobile/ IPAD, Data card etc. are provided to eligible employees by written recommendation from their HODs, where job or business needs demand immediate access to an employee for work-related communications. Notwithstanding the reason that is presented, head of the institution shall finally approve the request.

Employees in possession of Company devices are expected to protect the equipment from loss, damage or theft. Upon resignation or termination of employment, or at any time upon request, the employee may be asked to produce the device for return or inspection.

Occasionally, a device may be temporarily issued to an employee who is assigned to carry out vital Company business. Under all situations the policy and its guidelines are meant to be adhered to.

All the equipment’s issued remain the property of the company and not of particular individuals, teams or departments.

It shall be ensured by owners of mobile devices that no official data is stored in the privately used mobile device. Company provided mobiles and laptops shall be encrypted using appropriate cryptographic techniques on need & confidentiality basis. Regular backups shall be taken for devices carrying important, sensitive or critical business information. It shall to be ensured that employees using mobile devices are trained and made aware of the risks and also the controls that have to be implemented.

The authority for installation of software on the mobile device lies with the IT Team based on approval from CISO.

 Cryptographic controls and key management followed within the company shall follow national and applicable international legislations.

# 2.  Encryption and Key Management controls:

Where possible, all restricted, confidential and strictly confidential information shall be stored on a secure network server with restricted access. Where it has been deemed necessary by a Functional head to store restricted, confidential or highly confidential information on any device other than a network server the information must be encrypted.

**Desktop Computers**

Desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However the following types of desktop computers will need to have encryption software installed:

* Desktop/Laptop computers used by any staff to work from home (Teleworking).
* Desktop/Laptop computers which are located in unrestricted areas which are open to the public (if any).
* The preferred method of encryption for such Desktop computer devices shall be whole disk encryption.

**Laptop, Mobile Computer & Smart Devices**

All laptops shall have approved encryption software installed prior to their use within the secure area. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.

The preferred method of encryption for laptop computers, mobile computer devices and smart devices shall be whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all restricted, confidential and highly confidential information stored on the device.

Laptop, mobile computer devices and smart devices shall not be used for the long-term storage of restricted, confidential and highly confidential information.