Cryptography and Data Transmission Policy

1. INTRODUCTION

This policy is a sub policy of the Information Security Policy and establishes minimum requirements for endpoint security controls to protect Sensitive University Data or hereinafter referred as "sensitive data", store in rest and in transit. This is important to maintain integrity of the data and protect the confidentiality of the sensitive data from unauthorized access, stolen, getting lost or being intercepted.

2. SCOPE

This policy applies to all Sensitive University Electronic Data, such as personal data and examination data, stored in any non-centrally managed devices or transmitted over public networks or in relation to the University's network.

3. POLICY STATEMENT

All the University users shall make sure that sensitive data, storing on non-centrally managed electronic storages, endpoint devices at rest and transmission over a public network is encrypted.

Leakage of sensitive data can lead to serious consequences to the affected parties and the University. If data leakage is caused by a person overlooking, negligence, or improper protection, the person will be held fully responsible.

4. POLICY DETAILS

The storage of sensitive data on any devices used for University business shall be:

- limited to the minimum data necessary to perform the business functions;
- stored only for the time period required to make the business function;

Devices and Media Requiring Encryption

Where possible, encryption is required for all office computers, notebooks, mobile devices and portal storage drives that may be used to store or access Sensitive University Data.

Regardless of the storing media, when storing of sensitive data record(s) the media has to be employed proper encryption method as listed below:

- Office computer: File(s) storing sensitive data records should be encrypted
- Centrally managed networked drive: File(s) holding sensitive data records should be encrypted
- Portable storage: File(s) storing sensitive data records have to be encrypted
- Optical device: File(s) storing sensitive data records must be encrypted before storing on the optical device
- Public cloud storage: Drive(s), folder(s), file(s) and zip(s) storing sensitive data records must be encrypted prior to storing on the public cloud

Secure Data Transmission

Where possible any transfer of unencrypted sensitive data should take place via an encrypted channel to prevent interception and alteration. If encrypted connection is not feasible, the sensitive data should be encrypted before sending over an unencrypted network.

For transfer, including a clear-text password to access the data, the password should be transferred out of bounds, such as calling the recipient to provide the password. If alternative means are not feasible, the password has to be exchanged in a separate transmission.

The requirements for specific secure data transmissions are outlined as follows:

- ***Electronic Mail (Email)***
  Sensitive data shall be enclosed in an encrypted attachment when sending through email. The accompanying message and the file name must not reveal the contents of the encrypted file.

- ***Web***
  In assessing sensitive data through web browser, a secure protocol, such as *Secure Hypertext Transfer Protocol (HTTPS)*, should be established.

- ***Data File Transfer***

In exchange file containing sensitive data, the file has to be either encrypted or transferred over a secure network channel, such as *Secure Standard File Transfer Protocol (SFTP)*, or *Secure Shell (SSH)*.

- ***Remote Connections to Campus Network***
  Whenever connect from remote connections to the campus network to access and process sensitive data, such as Banner data, the channel has to be encrypted via a secure channel, for example access through *Virtual Private Network (VPN)*.

- ***Remote Access to University Production Servers***
  Remote access to the University production server console has to be over a reliable, secure tunnel, such as *Secure Shell Protocol (SSH)*.

  Any insecure protocols, such as *Telnet*, *rlogin*, and *FTP* are prohibited from accessing University's production environment.

5. ASSISTANCE

To support the implementation of this policy, ITSC provides centralized encryption software and provides install, configurations, and support to all eligible staff members. Departments or individual staff may approach ITSC for assistance.

6. REFERENCES

Information Security Policy, *http://www.ln.edu.hk/itsc/policy/it-policies-regulations*

7. APPROVAL

This policy has approved by the Teaching, Learning and Information Services (TLIS) Management Board on 19 May 2015.