Data Security

Data security generally refers to the prevention of unauthorised access by means of data encryption and setting of access right for individual users.

Organisations should pay attention to the following regarding data security:

- Data classification
- Data and file encryption
- Data backup and recovery
- Information disposal

Data Classification

Before implementing data security measures, all data must be categorised into different classifications according to its sensitivity and importance, e.g. general information, restricted information, confidential information etc. After data classification, draw up protection measures corresponding to the security requirements for different classifications. Generally, staff will need to obtain authorisation before they can access different kinds of classified information.

Data and File Encryption

Data encryption refers to the conversion of certain definite comprehensible messages into a bunch of illegible and obscure text. It can enhance confidentiality in transmitting and storing data and files.

Data Backup and Recovery

Set up an effective backup system to facilitate recovery of original data in case of system failure, inadvertent data deletion or illicit tampering. This will ensure the availability and integrity of data and software.

At the same time, audit tracking, network protection and other measures should also be implemented to further enhance information security.

Information Disposal

Before disposing or re-using a storage medium, all information and data previously stored must be erased completely using secure deletion methods to prevent possible data leakage. Secure deletion methods include using secure deletion software, degaussing or physical destruction etc.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk