Physical Security

Physical security is generally related to site preparation, equipment security and physical access control of a system. It aims to enhance the security level through housekeeping measures and proper staff training so that the impact of natural and man-made calamities can be reduced.

Site Preparation

Site preparation is the first and most important thing to do in physical security. Since most critical IT equipment is generally housed in the server room, careful site preparation for the server room is very important. Site preparation generally includes the following aspects:

1. The location of the server room and the security specifications;
2. Air conditioning (atmosphere), fire control (fire);
3. Flood control (water), power supply (electricity); and
4. Server room access control mechanism.

Housekeeping

Draw up guidelines on server room and system operation. For example, the server room must be kept clean and smoking, eating and drinking should be prohibited. Facilities related to “atmosphere”, “fire”, “water” and “electricity” should be maintained and tested regularly. Emergency exits should be checked regularly to ensure no blockage at any time. Hazardous or inflammable substances should be stored at a secure location. Fire extinguishers should also be put at a proper location in the server room.

Regular fire drills should be carried out to ensure that relevant staff is familiar with the proper emergency procedures in case of fire. Portable electronic devices must be used properly and stored securely in order to avoid information leakage.

Equipment Security

Equipment security refers to security measures related to the operation and disposal of computer hardware and equipment. It includes certain areas:

- Regular inspection of IT equipment.
- Back up critical information and store the backup media at a safe distance from the equipment. Unauthorised access to the backup media must be prohibited;
- The cases for carrying the media should have certain protection functions, such as fireproof, waterproof and anti-magnetic features.
- All sensitive information must be completely erased before disposal or re-use of computer equipment.

Physical Access Control

Unauthorised access to the area for handling sensitive information must be strictly prohibited. Proper physical access control should be considered to prevent unauthorised access. For example, use password to ensure that only authorised personnel are allowed to access the system. Access log should also be checked regularly and stored carefully. All maintenance work must be properly recorded, and all outsider workers must be under supervision.

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