Data Security

Chapter 4

Secure Data Management

LEARNING OBJECTIVES

1. Recognize ways of ensuring physical security of devices.
2. Recognize the importance of having a back-up procedure, and restore backed up data.
3. Distinguish between deleting and permanently destroying data.

PHYSICAL SECURITY OF DEVICES

- Security of data and information is not just an electronic function.
- Equipment and devices have to be locked away securely, with proper access control in place.
- Different ways of physical security of devices include the following:
  - **Log Equipment**
  - **Cable Locks**
  - **Access Control**

BACK-UP PROCEDURE

- A proper backup procedure is essential, for both business & personal users.
- It is best to schedule backups frequently.
- **Incremental backup** means only backing up files that have been modified since the last **full backup**.
- There are numerous methods of backups:
  - **Back-up to a device**
  - **Remote Backup Service (**AKA **Cloud Backup)**

PERMANENTLY DELETING DATA

- Deleting data from devices or drives means to remove it permanently.
- There are two main reasons for deleting data:
  - **Save Space**
  - **Security**

DELETING AND PERMANENTLY DESTROYING DATA

- When data is deleted it is moved to the Recycle Bin, once the Recycle Bin is emptied, the files are permanently deleted

COMMON METHODS OF PERMANENTLY DESTROYING DATA

- For security purposes, it is best to completely destroy data to ensure it can never be retrieved.
  - Shredding
  - Drive/ Media Destruction
  - Degaussing
  - Data Destruction Utilities