Chapter 4:: Secure Data Management

→ Physical Security of Devices
- Security is not just electronic physicall protection is equally important
- Physical Security ways:
  - Log Equipment
  - Cable Locks (computer lock)
  - Access Control (Security cards, biometric scanners)

→ Backup Procedure
- Why backup is critical
  - Computer crash
  - hard disk Failure
  - natural disasters
  - Electrical problems
  - human error
- Backup Scheduling Recommendation
  - Frequently (at least once a week)
  - Critical data / financial records : daily backup
  - Store backup devices in different location (off-site)
- Incremental Backup: only files modified since last full backup

→ Backup Methods
1) Backup to a Device
- Tape drives
- external hard disk
- USB drives
- Backup device should be off-site
- For both short/long term use

2) Remote Backup (Cloud)
- Automatically collects, compresses, encrypts data
- Transfers data to remote backup service provider's servers

→ Secure Destruction
Deleting ≠ Permanent Removal
- files moved to recycle bin first
- even "permanently deleted" files can be retrieved with special softw
→ Methods:
1) Shredding (physical destruction)
2) Drive/Media Destruction (physical destruction of a drive)
3) Degaussing (remove magnetic field from a device)
4) Data Destruction Utilities: software that can destruct data on a disk without harming it (Disk Scrubber)