UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 3

Always A Pioneer, Always Ahead

Information Security Control

Dr. Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

By the end of the lesson, the student will be able to:

a. understand the category of information security control
b. understand the types of information security controls
c. design a secure architecture based on information security control

CONTENT

- Introduction
- The objective of Information Security Implementation
- What is the information to secure?
- Information Security Controls
  - Perimeter Defense in Computer Network / IT
  - Category of Information Security Controls
    - Physical Control
    - Technical Control
    - Administrative Control
  - Types of Information Security Control
    - Directive , Preventive, Detective, Corrective and Recovery.
  - Designing an Information Security Control

INTRODUCTION

INTRODUCTION

Information Security Control is defined as:

(what?)

To safeguard the physical property, information, computer systems or other assets in the company.

(when?)

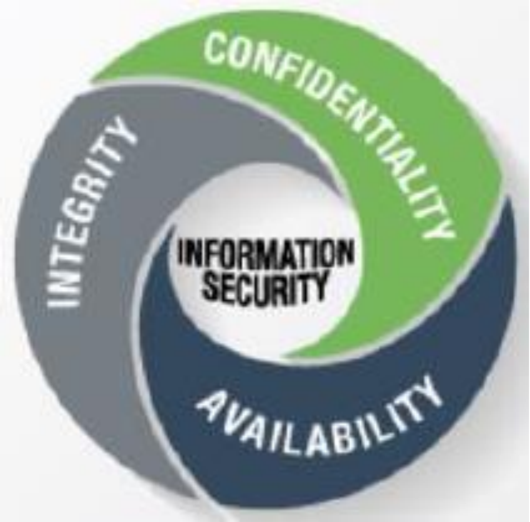
The implementation of **countermeasure** is done **before, during, and after the configuration and development controls** of **assets** in the organization **to minimize security risks** and **detect the potential threats or attacks**.

(how?)

Steps or procedures taken through standard to protect the confidentiality, integrity and availability of the information.

THE OBJECTIVE OF INFORMATION SECURITY IMPLEMENTATION

INFORMATION SECURITY OBJECTIVES



Fundamental Objectives of Information Security: The CIA Triad

- Confidentiality
  - “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” (44 USC Sec. 3542)
- Integrity
  - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 USC Sec. 3542).
  - Data Integrity
  - System Integrity
- Availability
  - “Ensuring timely and reliable access and use of information.” (44 USC Sec. 3542)

WHAT KIND OF INFORMATION TO SECURE?

EXAMPLES OF INFORMATION SYSTEM

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defences
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Tests

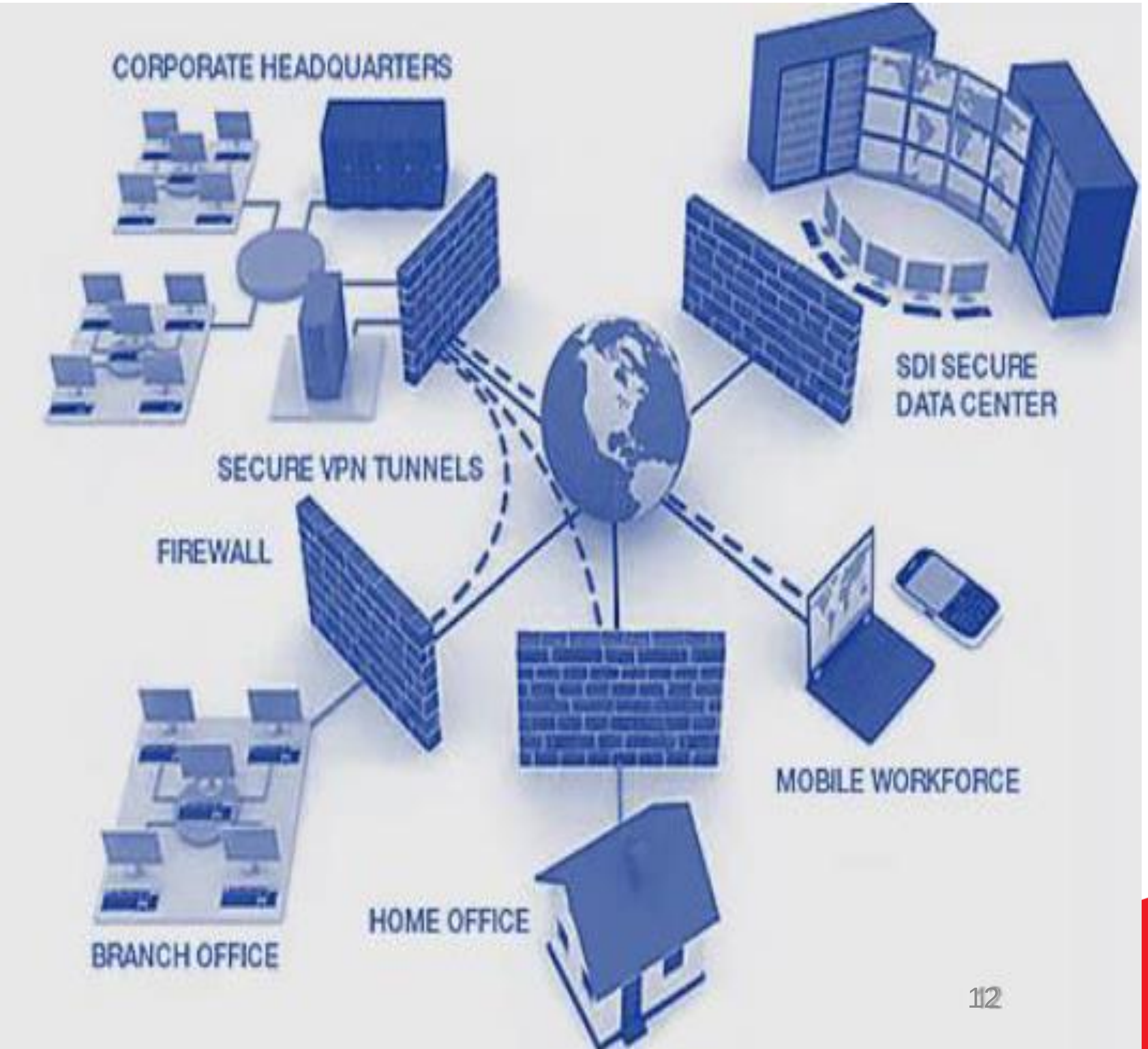
INFORMATION SECURITY CONTROLS

- Information security control defines the perimeter defenses, control categories and type of controls to be implemented in the organization.
- Each of category control needs a suitable type of controls application.
- For example, standard temperature in (Heating, Ventilation, Air and Conditioning) HVAC room. This look like a technician is in charge under technical control category. The task is to install, maintain and repair. Type of control suitable for this task is corrective.

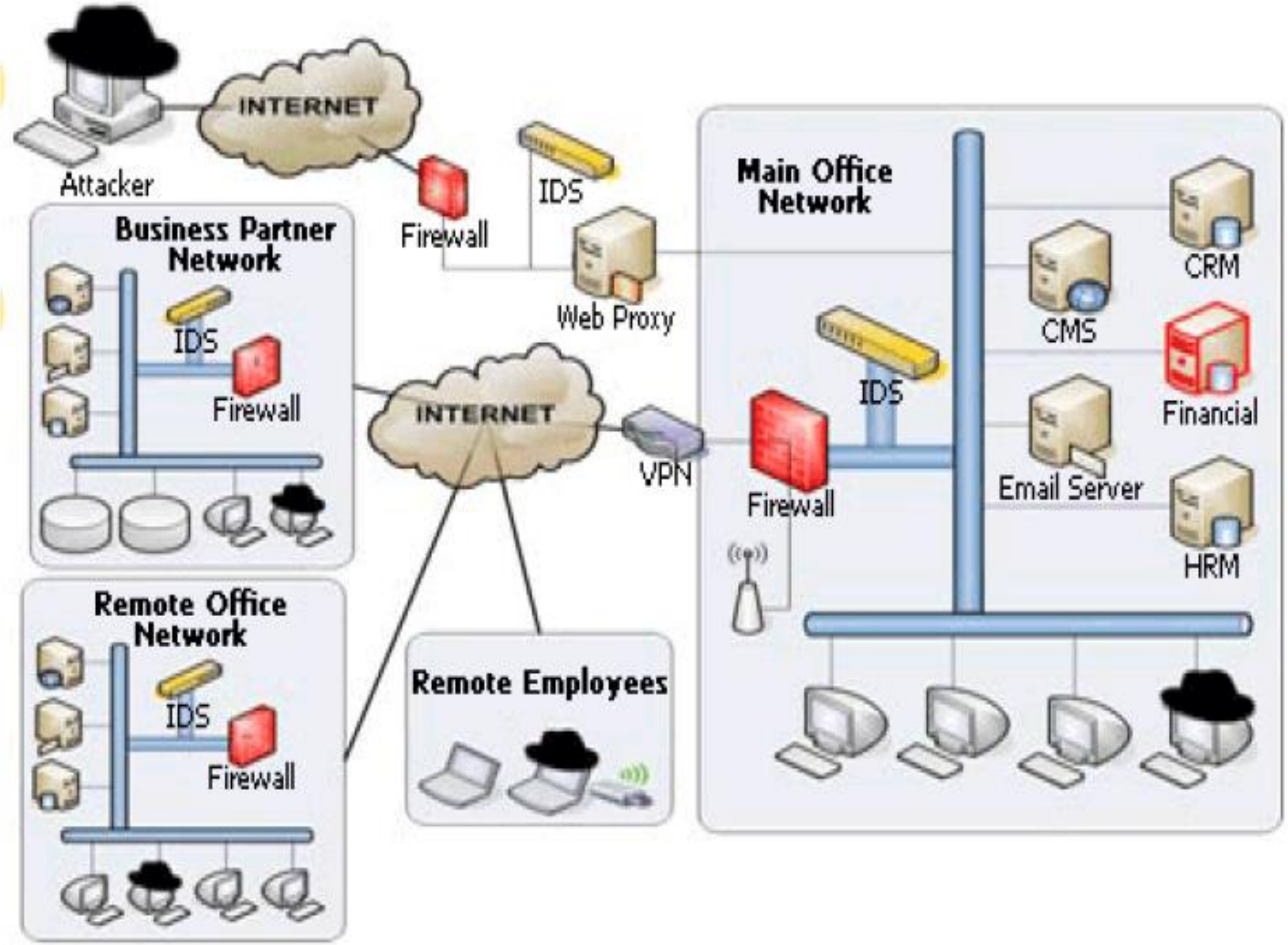
PERIMETER DEFENCES

PERIMETER DEFENCES

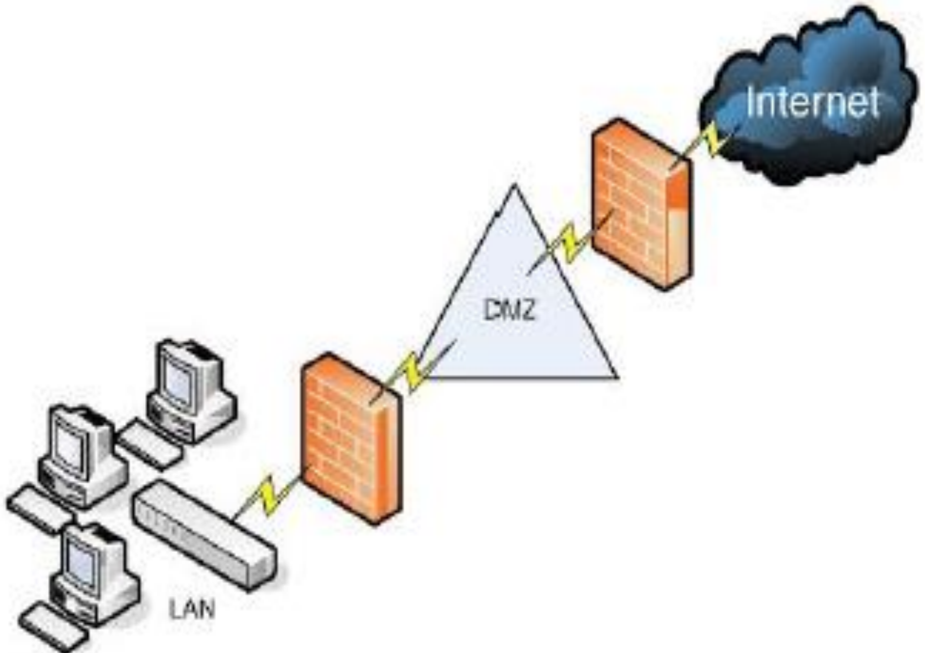
- The first line of control is perimeter defense at the remote location, to prevent unauthorized access to the IT assets.
- Perimeter defense has two modes:
  - Normal facility operation
  - Facility closed operation



PERIMETER DEFENCES



- Example of perimeter defenses technology are DMZ, firewalls (ASA), intrusion detection system (IDS), intrusion prevention system (IPS), proxies, and virtual private network (VPN).



CATEGORIES OF INFORMATION SECURITY CONTROLS

- Physical (Operational) Control
- Technical (Logical) Control
- Management (Administrative) Control

CATEGORIES OF INFORMATION SECURITY CONTROLS

- Operational (and Physical) Controls
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
    - Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Guards, Dogs
- Technical (Logical) Controls.
  - Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - Service Providers: Enterprise Architect, Security Engineer, CERT, NOSC, Helpdesk
- Management (Administrative) Controls
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management

PHYSICAL CONTROL

- The use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself.
- Besides, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster.

PHYSICAL CONTROL

- Physical controls serve to reduce risk of loss by:

1. denying unauthorized access.
2. deterring or discouraging attempts to gain unauthorized access.
3. delaying those who attempt to gain unauthorized access.
4. detecting threats, both criminal and non-criminal.

PHYSICAL CONTROL

- Implement physical security
- Where are they needed?
  - At perimeter and building grounds
  - At building entry points
  - Inside the building offices or rooms
  - For data centers or servers room security
  - Computer equipment protection

PHYSICAL CONTROL

- Physical security (facility or infrastructure protection)
- Element of physical - security badges, restricted areas, lights, access control system, fences, intrusion detection systems and danger sign or egress.
- Function of physical security deter, detect, delay and respond

TECHNICAL CONTROL

- Involves the use of safeguards incorporated in computer hardware operations or applications software, communications hardware and software, and related devices.
- Technical controls are sometimes referred to as a logical controls.
- Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Example of controls such antivirus software, passwords, encryptions.

TECHNICAL CONTROL

Example..

- Access controls system
- Identification and authorization
- Confidentiality
- Integrity
- Availability
- Non-repudiation

TECHNICAL CONTROL

Example..

- Environmental control area electrical power, fire detection and suppression, heating, ventilation , air and conditioning (HVAC).
- Fire protection control system (monitoring system to send alert to fire brigade to stop the fire).

ADMINISTRATIVE CONTROL

- Consists of management constraints, operational procedures accountability procedures and supplemental administrative controls established to provide an acceptable level of protection for computing resources.

- In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

ADMINISTRATIVE CONTROL

- Preventive administrative controls are personnel-oriented techniques for controlling people’s behavior to ensure confidentiality, integrity and availability of computing data and programs.

- Example of preventive administrative control include security awareness, technical training, supervision and disaster recovery.

ADMINISTRATIVE CONTROL

- Policies
- Standards
- Processes
- Procedures Guidelines
- Administrative entities (executive level, mid-level admin)

ADMINISTRATIVE CONTROL

- The purpose of Administrative Control are:
- Ensure organizational policies, procedures and standards are enforced.
- Segregation of functions to reduce errors and fraud.
- Supervision of personnel to ensure policies and procedures are being adhered to.

ADMINISTRATIVE CONTROL

- Pre-employment screening - employment, references and educational history check, background investigation and medical health check-up.
- On-going employee checked - security declarations, ongoing employee ratings or review by supervisors awareness program.
- Post-employment procedures - exit interview, termination of network access, closing the email's account, return the company's assets (such as ID and computer) and settle any debts in the organization before leave.

TYPES OF SECURITY CONTROL

- **Directive Controls** Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- **Preventive Controls** Included in preventive controls are physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- **Detective Controls** Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- **Corrective Controls** Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- **Recovery Controls** Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state

DESIGNING INFO. SEC. CONTROL

- Choosing a secure site…
  - Visibility - Low or high visibility?, type of neighbors, marks on the building
  - Local consideration - near hazard waste dump area, local crime rate
  - Natural disasters - heavy snow, earthquake zone
  - Transportation - excessive highway, air or road traffic in area

DESIGNING INFO. SEC. CONTROL

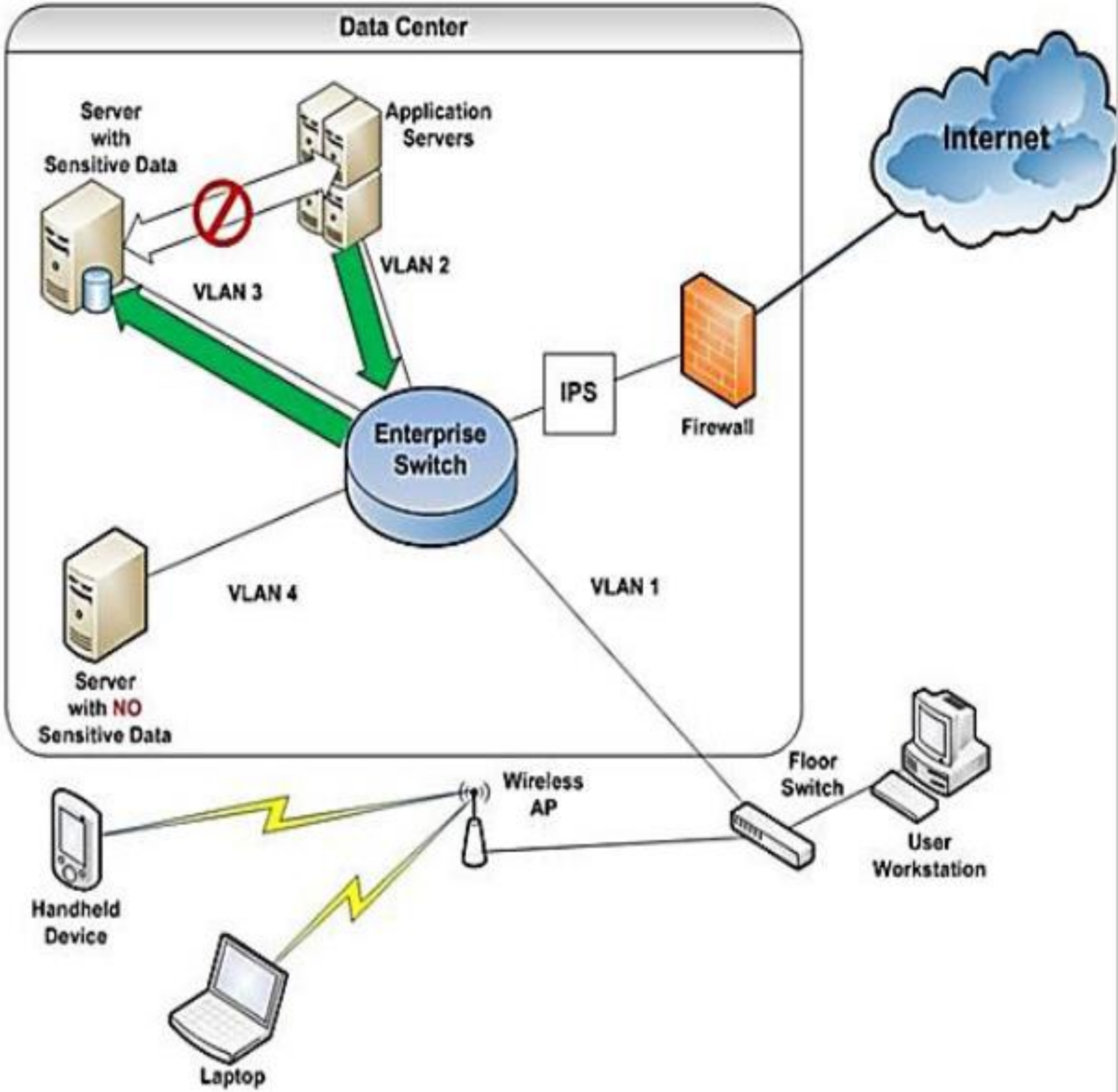
- Designing a secure site…

  - Walls - walls must have acceptable fire rating
  - Ceiling can they bear the right weight?, acceptable fire rating
  - Floors - Slap, raised
  - Doors - must have resist force entry, clear marked and alarmed emergency exit, hinges hidden internal or fixed
  - Windows should prevent any view, types

EXERCISE

- What is the type of control involved in the diagram?

- Answer :

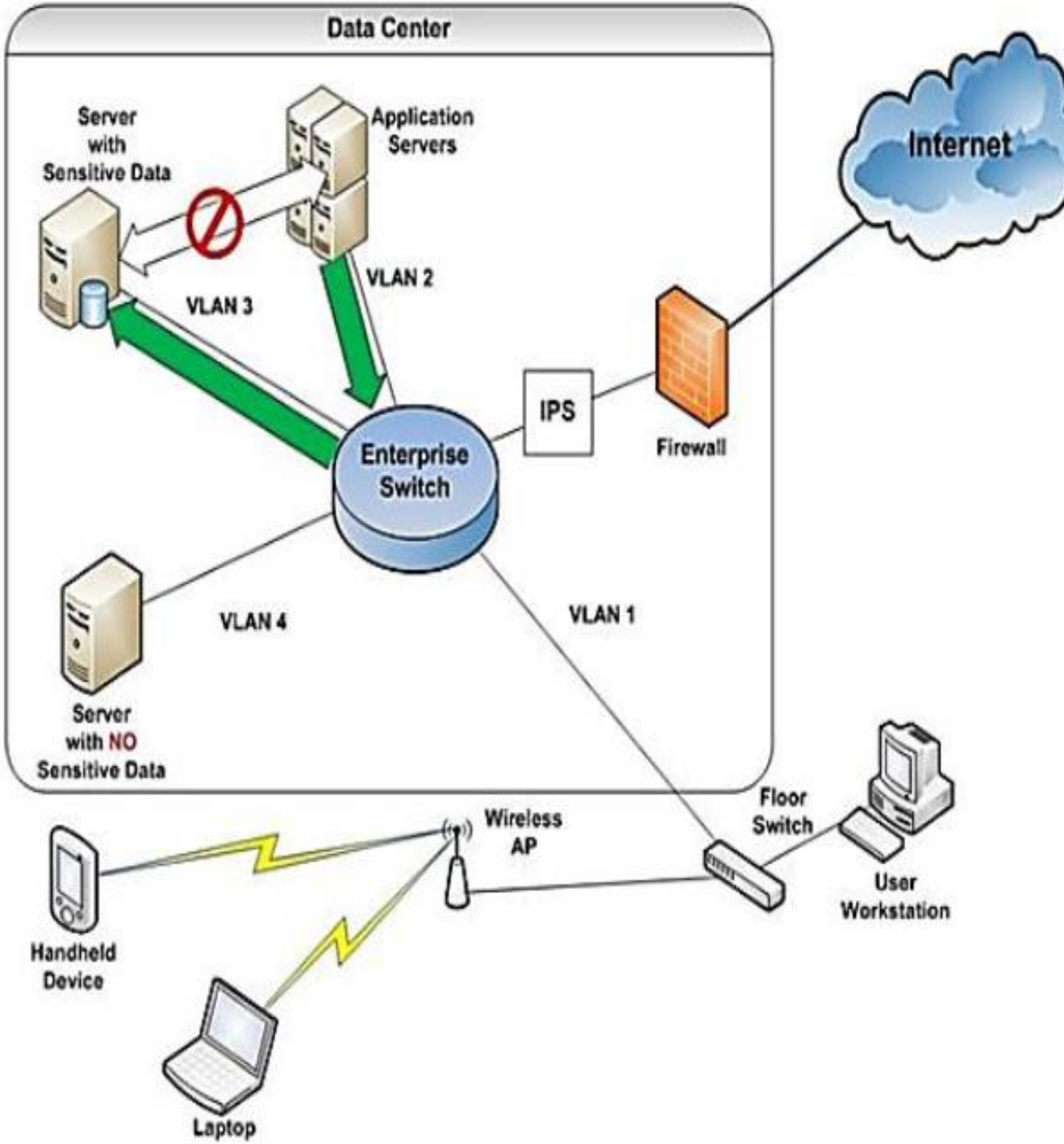


EXERCISE

- What is the type of control involved in the diagram?
- Answer :

1. Detective and Preventive under Technical Control - secure sensitive data at server from naughty employee and allow for the good employee to use the data for processing.

2. VLAN 4 has no sensitive data. User device is blocked from VLAN 3. Only VLAN 1 and VLAN 2 is available for user to access application server. User needs to register to access to application server and the pwd has an encryption.



Thank You

MyUTeM

www.utem.edu.my