PONDICHERRY UNIVERSITY

(A CENTRAL UNIVERSITY)

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

M.SC.COMPUTER SCIENCE

PONDICHERRY UNIVERSITY

NAME : PRATHIBA P

REGISTER NO : 23370085

SEMESTER : 3rd SEMESTER

SUBJECT : ISM (IT Asset management assignment)

S.no	Asset
1	PERSONALCOMPUTER
2	PATCHCABLE
3	PROJECTOR
4	SMART BOARD
5	BIOMATRIC SCANNER
6	UPS
7	CISCOWIRELESSACCESSPOINT
8	HDMICABLE
9	PRINTER(CANON)
10	CCTV

PERSONAL COMPUTER
(SYSTEM NO.49)

ABOUT:

A personal computer, often referred to as a PC, is a computer designed for individual use. It is typically used for tasks such as word processing, internet browsing, email, multimedia playback, and gaming. Personal computers are intended to be operated directly by an end user, rather than by a computer expert or technician. Unlike large, costly minicomputers and mainframes, time-sharing by many people at the same time is not used with personal computers.

Tech Specs:

Processor

12th Gen Intel® Core™ i3-1215U (10 MB cache, 6 cores, 8 threads, up to 4.4 GHz Turbo)

Operating System

Windows 11 Home Single Language, English

Video Card

Intel® UHD Graphics

Display

15.6", Non-Touch, FHD 1920x1080, 120Hz, WVA, Anti-Glare, 250 nit, Narrow Border, LED-Backlit

Memory

8 GB: 1 x 8 GB, DDR4, 2666 MT/s

Storage

512GB M.2 PCIe NVMe Solid State Drive

Color

Carbon Black

Microsoft Office

Microsoft Office Home and Student 2021

Security Software

McAfee Live Safe 5-device 1-year

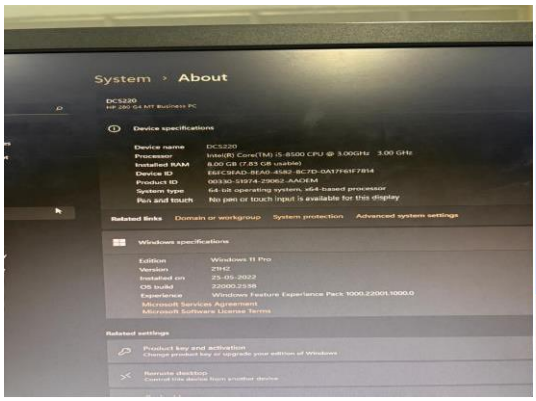
Support Services

1Y Basic Onsite Service after remote diagnosis with Hardware-Only Support

Accidental Damage Protection

NONE

<u>Network information:</u>



Ethernet Adapter Ethernet 1

- Description: Real tekPCI e GBE Family Controller
- Physical Address (MAC):C4-65-16-21-C1-CA
- IPv4 Address:10.10.32.37(Preferred)
- Subnet Mask:255.255.254.0
- Default Gateway :10.10.31.8
- DNS Servers :8.8.8.8, 10.14.139.5

Ethernet Adapter Ethernet 2 (Virtual Box Host-Only)

- Description: Virtual Box Host-Only Ethernet Adapter
- Physical Address (MAC):A4-00-27-00-08-09
- IPv4 Address:192.168.63.1(Preferred)
- Subnet Mask:255.255.255.0

Wireless LAN Adapter Wi-Fi

- Description: RealtekRTL8821CE802.11acPCIeAdapter
- Physical Address(MAC)**:A4-FC-77-24-61-E7
- Media State: Disconnected

RISK	VULNERABILITIES
· **Data Loss**: Accidental deletion, hardware failure, or software corruption can lead to the loss of critical lab data. · **Cyber security Threats**: PCs are vulnerable to malware, ransom ware, and unauthorized access, potentially compromising sensitive data. · **Physical Damage**: Equipment can be damaged due to mishandling, spills, or power surges, affecting functionality	· Weak password sand lack of multi-factor authentication · Out dated operating system sand software · Unlatched security vulnerabilities · Lack of firewall and antivirus protection · Inadequate network security (e.g., open or unsecured Wi-Fi) · Physical access vulnerabilities (e.g., unlocked workstations)
MITIGATION · **Cyber security**: Mitigating risks associated with personal computers (PCs) in terms of malware, data breaches, or security vulnerabilities. · **Environmental Science**: Mitigation strategies related to the environmental impact of personal computers and technology. · **Finance or Economics**: Mitigating financial risks associated with personal computing, like data loss or unauthorized access to financial information.	**ASSET MANAGEMENT POLICY** · **PC Inventory Management**: All personal computers (PCs) must be registered in an asset inventory, including details like serial numbers, owners, and locations. Regular audits should be conducted to keep this information current. · **Security Measures**: PCs must have up-to-date antivirus software, enabled firewalls, and security patches applied promptly. Access should be secured with strong passwords and multi-factor authentication.

REFERNCE:

NISTSP800-53-Security and Privacy Controls for Information Systems and Organizations

PATCH CABLE

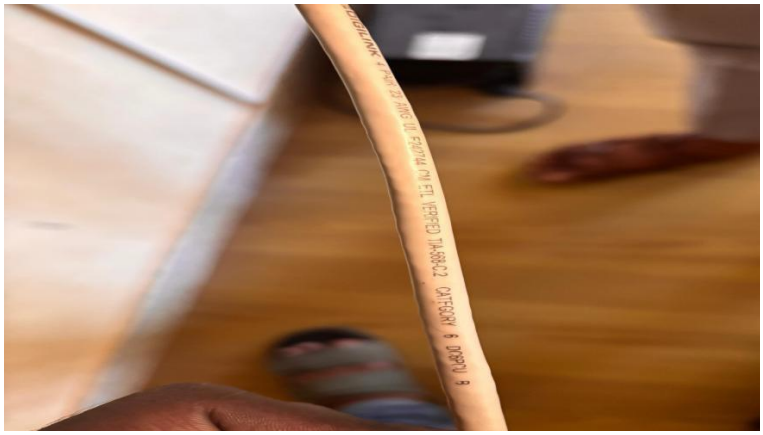
ABOUT:

A patch cable, patch cord or patch lead is an electrical or fiber-optic cable used to connect ("patch in") one electronic or optical device to another for signal routing. Devices of different types (e.g., a switch connected to a computer, or a switch to a router) are connected with patch cords.

Features:

- CAT6A foil-screened twisted pair (FTP, aka F/UTP) shielded patch cable
- 650 MHz high-bandwidth design supports 10GBASE-T at 100 meters (330 feet)
- Flexible 26 AWG stranded FTP wire
- Molded PVC jacket with low-profile snagless boot for added durability
- Future-proof and reverse compatible with CAT6/CAT5e
- Fully certified to 10GBASE-T TIA/EIA-562-B.2-10 specifications
- True shielded CAT6A rated RJ45 connectors with gold plated contacts
- ISO/IEC compliance reduces near end cross talk (NEXT) by 3 dB (50%)

- Integrated x-type pair separator further reduces interference from cross-talk
- 100% foil shield coverage for excellent alien cross talk (ANEXT) rejection
- 28% smaller diameter than unshielded (UTP) CAT6A cables



RISK	VULNERABILITIES
• **Connection Failure**: Patch cables are susceptible to wear and tear, which can lead to connection issues and disrupt network communication. • **Data Interception**: Unsecured or damaged cables may allow unauthorized access to transmitted data. • **Physical Damage**: Patch cables can be damaged by foot traffic, spills, or misplacement ,impacting functionality.	• **Cable Wear**: Constant plugging and unplugging, or improper handling, can cause cable degradation. • **Unsecured Connections**: Patch cables not properly secured can result in network disruptions. • **Environmental Exposure**: Exposure to extreme temperatures, moisture, or chemicals can deteriorate the cable's integrity.
MITIGATION	**ASSETMANAGEMENT POLICY**
• **Regular Inspection**: Periodically inspect patch cables for any signs of wear or damage and replace them if needed. • **Proper Cable Management**: Implement cable management practices to prevent tangling and damage. • **Environmental Protection**: Use cable covers or conduits to shield cables from environmental hazards and reduce physical wear	• **Inventory Management**: Label each patch cable and record it in aninventorywithinformationlike type, length, location, and purchase date. • **Maintenance Schedule**: Include patch cables in regular audits and maintenance schedules to ensure they are functional and properly connected. • **Security Measures**: Ensure all cables are securely connected to prevent accidental disconnections and unauthorized access to the network.

REFERNCE:

- ISO55001:2014,
- ISO/IEC 27001:2013
- ISO55001:2014,

PROJECTOR

ABOUT:

A projector or image projector is an optical device that projects an image (or moving images) onto a surface, commonly a projection screen. Most projectors create an image by shining a light through a small transparent lens, but some newer types of projectors can project the image directly, by using lasers. A virtual retinal display, or retinal projector, is a projector that projects an image directly on the retina instead of using an external projection screen.

SPECIFICATION:

Type of display	Poly-silicon TFT active matrix
Resolution	**Bright Link 480i**: 1024 × 768 pixels (XGA)
	Bright Link 475Wi/485Wi: 1280 × 800 pixels (WXGA)
Lens	F= 1.80
	Focal length: 3.71 mm
Color reproduction	Full color, 16.77 million colors
Brightness	**BrightLink 475Wi**:
	Normal Power Consumption mode:
	White light output 2600 lumens (ISO 21118 standard)
	Color light output 2600 lumens
	ECO Power Consumption mode:
	White light output 1800 lumens (ISO 21118 standard)
	Bright Link 480i:
	Normal Power Consumption mode:
	White light output 3000 lumens (ISO 21118 standard)
	Color light output 3000 lumens
	ECO Power Consumption mode:
	White light output 1800 lumens (ISO 21118 standard)

	Bright Link 485Wi:
	Normal Power Consumption mode:
	White light output 3100 lumens (ISO 21118 standard)
	Color light output 3100 lumens
	ECO Power Consumption mode:
	White light output 1800 lumens (ISO 21118 standard)
Contrast ratio	3000 to 1 with Auto Iris on and Normal Power Consumption mode

warranty:

Out of warranty.

RISK

- **Image Quality Degradation**: Dust accumulation on the lens or internal components may reduce image clarity.
- **Overheating**: Extended use without proper ventilation can lead to overheating, potentially damaging internal parts.
- **Electrical Surge**: Power surges may damage the projector's circuits, affecting functionality

VULNERABILITIES

- **Physical Damage**: The projector lens or housing may get damaged due to falls, knocks, or mishandling.
- **Unsecured Access**: Projectors with unsecured network connections are vulnerable to unauthorized access or tampering.
- **Firmware Vulnerabilities**: Outdatedfirmware canexposethe projector to security vulnerabilities, especially if connected to a network.

MITIGATION

- **Regular Cleaning**: Clean the lens and air filters periodically to maintain image quality and airflow.
- **Ventilation Check**: Ensure the projector is placed in a well-ventilated area to prevent overheating.

ASSETMANAGEMENT

- **Inventory Management**: Register the projector in the asset inventory , noting the model, serial number, location, and purchase date.
- **Maintenance Schedule**: Include the projector in routine maintenance schedules to check for dust buildup, firmware updates, and functionality.
- **Reference**: ANSI/TIA-568-C.2

New lines mart Board

ABOUT:

A Smart Board is an interactive whiteboard. It lets you control a computer using touch, a stylus, or gestures. Unlike traditional whiteboards, Smart Boards allow you to interact with digital content in real-time. You can write, draw, click, drag, and drop items just like you would on a tablet or smart phone.

SPECIFICATION:

HardwareSpecifications:

- **Device**: New line Smart Board
- **Display Resolution**: Likely 4K Ultra HD (common for New line models)
- **Operating System Compatibility** : Supports both Android and Windows
- **Touch Technology**: Multi-touch ,enabling multiple users to interact simultaneously

Software Specifications:

- **Android OS** :Built-in, allowing access to core features and applications without external devices.
- · **Windows OS**: Available when connected to an OPS (Open Pluggable Specification) computer or external device, offering a full Windows experience.

Network Information:

- **DNS Servers**:
    - Primary:8.8.8.8(Google Public DNS)
    - Secondary:14.139.5.5(local or custom DNS)

- Tertiary:4.2.2.2(Level3 DNS)

- **Wi-Fi Adapter** :Intel(R)Wi-Fi6AX201160MHz

    - **Status**: Disconnected
    - **Physical Address (MAC)**:5C-E4-2A-F7-BE-A8
    - **DHCP**: Enabled
    - **Auto-configuration**: Enabled

- **Additional Network Adapters**: Microsoft Wi-Fi Direct Virtual Adapter and Wi-Fi Direct Virtual Adapter#2

    - **Status**: Disconnected
    - **Physical Addresses (MAC)**:

        - Adapter1:5C-E4-2A-F7-BE-A9
        - Adapter2:5E-E4-2A-F7-BE-A8
    - **DHCP**: Enabled
    - **Auto-configuration**: Enabled

Mitigation	Vulnerabilities
• **Access Control**: Implement password protection and user roles to restrict access. • **Network Security**: Use WPA3 encryption and VPNs for secure connections. • **Regular Updates**: Enable automatic updates for OS and apps. • **Endpoint Protection**: Install antivirus and firewall on Windows OS. • **Data Encryption**: Encrypt stored files and use secure cloud storage	• **Unauthorized Access**: Risk of unauthorized users accessing settings or data. • **Malware Attacks**: Vulnerable to malware in Windows OS environment. • **Network Breaches**: Potential access by unauthorized devices. • **Data Leakage**: Risk of accidental exposure via unsecured cloud storage. • **Outdated Software**: Risk of exploits due to un patched vulnerabilities.
Risk	**Policies**
· **Unauthorized Access**: ·Risk of unauthorized users accessing sensitive settings, files, or networked resources on the smart board, leading to data breaches or misuse. · **Malware Infection**: ·The smart board, particularly with Windows-based OPS (Open Plug gable Specification) modules ,may be susceptible to malware or viruses if not properly secured, potentially compromising network security.	• **User Authentication Policy**: Require unique logins and enable two-factor authentication. • **Data Privacy Policy**: Limit access to sensitive data and enforce encryption. • **Acceptable Use Policy**: Define acceptable use and restrict unapproved app downloads. • **Incident Response Policy**: Set protocols for identifying and responding to security incidents. • **Device Management Policy**: Regularly update software and conduct system audits

REFERNCE:

- **ISO55000**:This standard provides an overview of asset management and outlines the principles and terminology.
- **ISO 55001**: This specifies requirements for an asset management system, helping organizations effectively manage their assets throughout their lifecycle.

BIO MATRIC SCANNER

ABOUT:

Biometric scanners in laboratories are advanced devices that identify individuals through unique biological traits, such as finger prints , facial features, or iris patterns. They enhance security by ensuring that only authorized personnel can access sensitive areas and equipment, reducing the risk of data breaches. Additionally, biometric systems improve operational efficiency by streamlining authentication processes, allowing quick access without the need for passwords or ID cards.

SPECIFICATION:

Hardware:

- ·**Model**:XYZ-500
- ·**Processor** :Dual-Core ARM Cortex A7
- ·**Memory**: 512MBRAM,4GBFlashMemory
- ·**Display**:3.5-inchTFTLCD,320x240 pixels
- ·**Bio metric Sensor** :Optical fingerprint sensor, 500DPI,storesupto10,000 templates
- ·**Card Reader** :RFID/MIFARE/EM, upto10,000cardtemplates
- ·**Network** :Ethernet(10/100Mbps),optional Wi-Fi(2.4 GHz)
- ·**Interfaces**:USB2.0,RS232/RS485
- ·**Power**:DC12V/1.5A,2000mAhbatterybackup

Software :

- ·**Software** :Linux-based OS, custom attendance software, HR/payroll integration support
- ·**Attendance Modes**: Fingerprint, Card ,Password, Face(optional)
- ·**Communication Protocols**: TCP/IP, USB-host,RS232/RS485
- ·**Operating Environment**:-10°Cto50°C,20%-80% humidity
- ·**Certifications**: CE ,FCC , RoHS

Risks	Vulnerabilities
• **Data Breaches** :Unauthorized access to biometric data can lead to identity theft. • **Spoofing Attacks**: Biometric systems can be tricked by fake fingerprints, facial recognition masks, or voice recordings. • **Privacy Concerns**: The collection and storage of biometric data raise significant privacy issues. • **System Failure**: Biometric systems may fail to recognize legitimate users, leading to denial of access	• **Insecure Storage**: Biometric data that is not securely encrypted can be exposed. • **Limited Authentication**: Some biometric systems may only use a single factor (e.g., fingerprints), making them less secure. • **User Behavior**: Users may share or expose their biometric traits, intentionally or unintentionally.
Mitigation Strategies	**Policies**
• **Encryption**: Ensure all biometric data is encrypted both at rest and in transit. • **Multi-Factor Authentication**: Combine biometrics with other authentication methods (e.g., passwords, tokens). • **Regular Audits**: Conduct periodic security audits and vulnerability assessments on biometric systems.	• **Data Protection Policy**: Establish clear guidelines on the collection, storage, and sharing of biometric data. • **Access Control Policy**: Define who has access to biometric systems and data, ensuring access is limited to authorized personnel. • **Incident Response Policy**: Create a protocol for responding to security breaches orincidents involving biometric data.

REFERNCE: ISO/IEC19795-1:2006,ISO/IEC29100:2011

UPS (Numeric Digital 1000 Plus-V)

About:

This is a Numeric Digital 1000 Plus-V uninterruptible power supply (UPS) designed to provide backup power and protect electronic devices from power fluctuations. It is rated for 1000 VA, suitable for supporting computers, networking devices, and other sensitive equipment. The UPS includes an automatic voltage regulator (AVR) to stabilize the output power during low or high voltage conditions. The LED indicators on the front panel show the operational status and battery charge level. Hardware feature typically include as e aled lead-acid battery, input and output ports, and cooling vents

SPECIFICATION:

Hardware Specifications

1. **PowerCapacity**:1000VA/600W,suitableforsupportingmultipledeviceslike computers, routers, and small servers.

2. **BatteryType**: Sealedlead-acidbattery,designed for long life and high reliability, with typically a 5–10 minute backup duration for moderate loads.

3. **Automatic Voltage Regulation(AVR)**:Stabilizes in coming power,protecting against surges, sags, and brownouts without depleting the battery.

4. **LED Indicator**: LED lights for indicating power status ,battery mode ,and faults, providing at-a-glance operational insights.

5. **Cooling System**: Ventilations lots to prevent verheating ,ensuring consistent performance and prolonged device life.

6. **Input / Output Ports**: Includes power input and multiple output sockets for connected devices, possibly with overload protection.

Software Specifications

1. **Power Management Software:** Compatible software (if provided or compatible with third-party UPS monitoring software) enables real-time monitoring and management.

2. Communication Interface: USB orserial connectivity for connecting the UP S to a computer, allowing automated actions like safe shutdown during extended outages.

3. Event Logging: Software may include options for logging events such as power outages, battery status, and system faults for easy troubleshooting.

4. **Battery Health Monitoring :**Real-time battery health and charge level monitoring to alert users of any issues

Self-Test Functionality :Software or on board controls may enable periodic self-tests to ensure battery health and overall UPS functionality.

.

Risks	Vulnerabilities
• **Power Outages:** Sudden loss of power can lead to equipment failure and data loss. • **Battery Failure:** Batteries may degrade over time, resulting in reduced runtime and reliability. • **Overloading:** Connecting more devices than the UPS can handle can lead to overheating and potential failure. • **Environmental Factors:** High temperatures ,humidity, or dust can affect UPS performance.	• **Aging Equipment:** Older UPS systems may be more prone to failures. • **Inadequate Capacity Planning:** Failure to assess future power needs can result in insufficient UPS capacity. • **Physical Access:** Unauthorized physical access to the UPS can lead to tampering or sabotage. • **Firmware Issues:** Outdated firmware can expose the system to security vulnerabilities
Mitigation Strategies	**Policies**
• **Regular Testing and Maintenance:** Schedule routine inspections and testing of the UPS and its batteries to ensure proper operation. • **Load Management:** Calculate and monitor the total load connected to the UPS, ensuring it does not exceed its capacity. • **Environmental Controls:** Install the UPS in a controlled environment with adequate cooling and dust filtration. • **Battery Replacement:** Establish a schedule for replacing batteries based on manufacturer recommendations or performance monitoring.	• **UPS Usage Policy:** Define guidelines for the appropriate use of UPS systems, including acceptable load limits and device connections. • **Maintenance Policy:** Establish a maintenance schedule that includes regular inspections, testing, and battery replacement. • **Incident Response Policy :**Outline procedures for responding to UPS failures or power outages, including communication plan sand escalation procedures. • **Access Control Policy:** Implement restrictions on physical access to UPS systems to prevent unauthorized tampering.

REFERNCE:

- ·ISO/IEC19795-1:2006,focusing on stand ardized performance testing and operation.
- ISO/IEC29100:2011,addressing aspects of privacy and security management relevant to network-connected UPS systems

CISCOWIRELESSACCESSPOINT

ABOUT:

Cisco wireless access point installed alongside a lighting fixture, likely providingnetworkcoveragewithinanindoorenvironment.Suchconfigurationsare essential for ensuring comprehensive wireless network connectivity in spaces like offices, schools, or other facilities. The integration of wired and wireless infrastructure with in a shared physical space reflects the effort to maintain network accessibility and support a variety of internet-enabled devices.

SPECIFICATION:

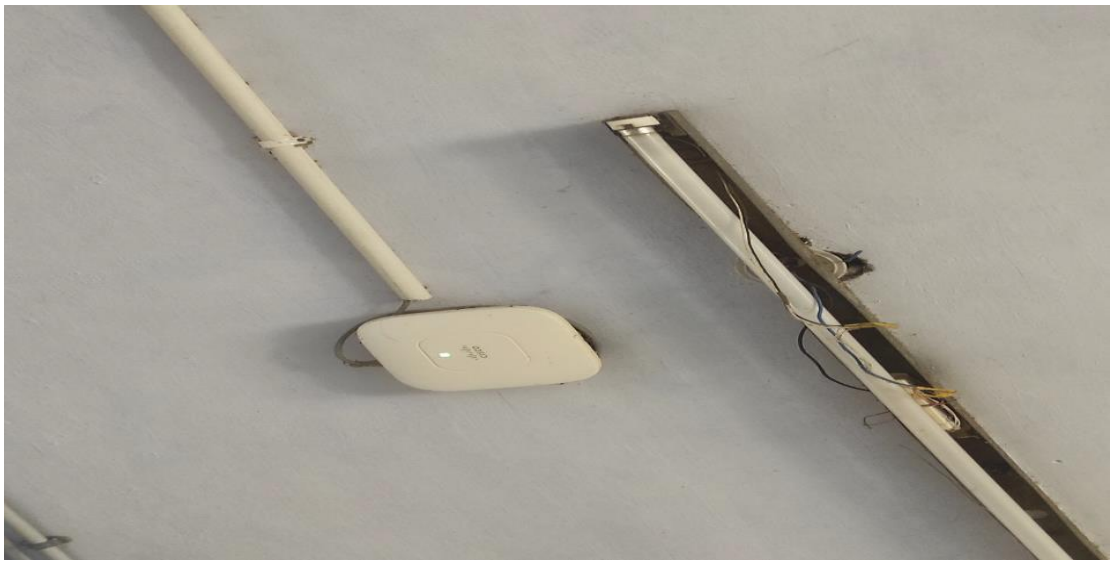
Hardware

- **Cisco Access Point(AP)**:Provides Wi-Fi coverage, powered via Ethernet (PoE).
- **Cabling:** Ethernet cables supply data and power, minimizing clutter.

Lighting Fixture Fluorescent tube near by; might cause minor interference.

Software

- **Cisco OS**: Powers the AP with features like user authentication and secure access.
- **Management Tool s:** Managed via Cisco DNA Center for monitoring, configuration, and security.
- **Security Features**: Supports WPA3,userauthentication, and network segmentation for protection.



Risks	Mitigations
• **Unauthorized Access**: Intruders may gain access to the network through unsecured or poorly configured WAPs. • **Data Interception**: Sensitive data may be intercepted without proper encryption. • **Firmware Vulnerabilities**: Outdated firmware increases the risk of exploitation. • **Network Overload**: Excessive connections can lead to performance degradation or outages. • **Physical Tampering**: Unauthorized physical access can lead to malicious reconfiguration or downtime.	• **Strong Authentication**: Implement WPA3 and restrict access using MAC filtering or enterprise authentication. • **Encryption**: Enforce WPA3 or stronger encryption standards to protect data. • **Firmware Updates**: Regularly update firm ware to protect against vulnerabilities. • **Load Management**: Monitor network traffic and apply load-balancing to handle peak usage. • **Physical Security**: Place WAPsin secure, limited-access areas to prevent tampering
Vulnerabilities	**Policies**
• **Outdated Firmware**: Increases susceptibility to known security exploits. • **Weak or No Encryption**: Inadequate encryption opens the network to data interception. • **Default Configurations**: Using default settings (e.g., SSID, passwords) creates potential security gaps.	• **Access Control Policy**: Require WPA3 or enterprise authentication for all connections; disable unsecured access. • **Firmware Management Policy**: Maintain an update schedule in alignment with Cisco's latest security patches. • **Encryption Policy**: Enforce WPA3 encryption; prohibit deprecated protocols (e.g., WEP). • **Network Segmentation Policy**: Segment guest and internal networks; disable SSID broadcasting on sensitive networks.

REFERNCE:

- **ISO/IEC19795-1:2006**:Aligning with standardized performance testing and security validation.

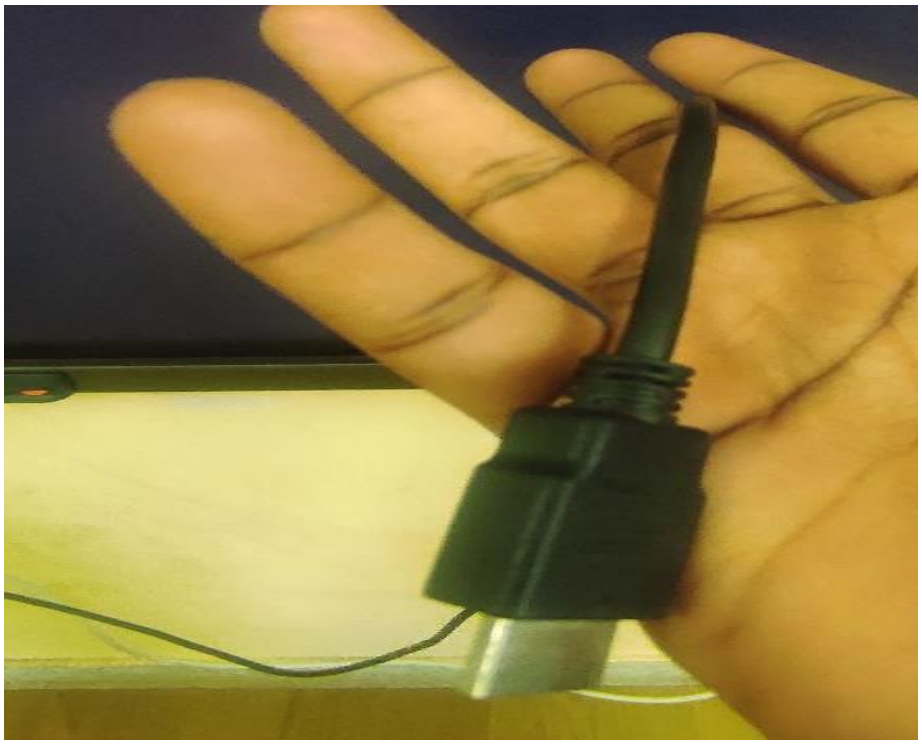
HDMI CABLE

ABOUT:

HDMI, or High-Definition Multimedia Interface, is a widely used technology for transmitting high-quality video and audio between devices. HDMI cables enable seamless connections between source devices(like gaming consoles, Blu-ray players, or computers) and display units (like TVs, monitors, or projectors), delivering both audio and video signals over a single cable. The HDMI standard was first introduced in2002 and has since evolved with various versions that offer increasingly advanced features.

SPECIFICATION:

- **Resolution**:Upto10K@120Hz(HDMI2.1).
- ·**Bandwidth** :48Gbpsmax(HDMI2.1).
- **Audio**: Supports Dolby True HD, DTS- HD, and upto 32 audio channels (eARC for higher fidelity).
- ·**HDR Support** :HDR10,DolbyVision,HDR10+.
- ·**VRR (Variable Refresh Rate)** :Reduces screen tearing, ideal for gaming.
- ·**Cable Types**:
  - *Standard*: Upto 1080p.
  - *High-Speed*: Upto4K@30Hz.
  - *Premium High-Speed*: 4K@60Hzwith HDR.
  - *Ultra High-Speed*: 4K@120Hz,8K@60Hz,required forHDMI 2.1.
- **Compatibility** :Backward compatible with older HDMI versions.



Risk	Mitigation
1. **Data Breaches**: Unauthorized access leading to loss or theft of sensitive information. 2. **System Failures**: Hardware or software malfunctions causing operational downtime. 3. **Phishing Attacks:** Attempts to deceive employees into revealing confidential information	1. **Encryption:** Protects data by converting it into a secure format, accessible only by authorized users. 2. **Access Control**: Limits user access based on roles to minimize exposure to sensitive information. 3. **Regular Security Audits**: Periodic assessments to identify and address vulnerabilities.
Vulnerability	**Policy**
1. **Outdated Software**: Lacks the latest security patches, making it prone to exploitation. 2. **Weak Passwords:** Increases the risk of unauthorized access to systems and accounts. 3. **Unsecured Networks:** Allows hackers to intercept data on unprotected connections.	1. **Access Control Policy**: Defines who has access to specific systems and data. 2. **Incident Response Plan**: Outlines steps for handling and reporting security incidents. 3. **Data Protection Policy:** Ensures data confidentiality, integrity, and compliance with regulations

PRINTER (CANON)

ABOUT:

The Canon image RUNNER series is designed for reliable, high-volume document handling, supporting functions such as copying, scanning, and printing. Known for their durability, these copiers are often found in office settings where consistent, efficient performance is needed. This specific model combines straight forward control with Canon's quality imaging technology, allowing users to handle typical document workflows effectively

Specifications:

Functionality:

1. Copying: High-r esolution document reproduction.
2. Printing: Support for monochrome printing.
3. ***Scanning*****:** Basics can functions for archiving or digital transfer.

Paper Handling:

1. Supports a variety of paper size sand types.
2. Has an automatic documen feeder for bulk copying.
3. Multiple paper trays to handle high-volume tasks.

User Interface:

1. Basic LCD display with physical buttons for operation.
2. Options for adjusting print and copy settings.
3. Simplified control panel, suitable forn on-technical users.

FEATURES:

- **Multi-Functionality**: Capable of copying, printing ,and basic scanning, making it a versatile choice for everyday office tasks.

- **User-FriendlyInterface**: Simple control panel with an LCDs creen and physical buttons, allowing easy access to core functions for users with minimal technical skills.

RISK	Vulnerabilities
• **Security Risks**: They can be hacked, leading to data breaches. • **Compatibility Issues**: They may not work well with all operating systems or software. • **High Supply Costs**: Ink and toner can be expensive.	• **Enhance Security**: Use strong passwords ,keep firmware updated, and configure security settings to prevent unauthorized access. • **Check Compatibility**: Before purchasing, verify that the printer is compatible with your operating system and software. Regularly update drivers as needed.

Mitigation	Policy
· **Enhance Security**: • Use strong, unique passwords for network access. • Regularly update the printer's firm ware to patch any security vulnerabilities. • Configure network security settings ,such as enabling firewalls and disabling unused services. · **Check Compatibility**: • Before purchasing a printer, verify compatibility with your operating system and software applications. • Regularly check for driver updates on the Canon website to ensure optimal performance	· **Security**: • Use strong passwords for printers. • Keep printer firmware updated. • Set up firewalls and disable unnecessary features. · **Compatibility**: • Check compatibility with systems before buying a printer. • Update printer drivers regularly. · **Supply Management**: • Use high-yieldink orto ner cartridges. • Get approval be for e using third-party cartridges. • Monitor printing volume to control costs

REFERNCE:

- **ISO/IEC 27001:2013** - Information security management systems — Requirements. This standard provides a framework for establishing, implementing, maintaining, and continually improving information security management with in the organization.

- **ISO 9001:2015** - Quality management systems — Requirements. This standard outlines the criteria for a quality management system, focusing on meeting customer expectations and delivering customer satisfaction.

CCTV (Closed -Circuit Television)

About:

CCTV(Closed-Circuit Television) systems play a vital role in enhancing security and monitoring within laboratory environments. These systems help ensure the safety of personnel, protect sensitive equipment, and secure valuable research data. By providing real-time surveillance and recording capabilities, laboratory CCTV can deter unauthorized access, monitor compliance with safety protocols, and support incident investigation. This document outlines the specifications and features of a typical laboratory CCTV system, emphasizing its importance in maintaining a secure and efficient working environment.

Specifications:

Model: Canon Network Security Camera(Model:VB-H43)

Camera Type:

1. **Type** :IP Camera
2. **Resolution**: 1920x1080(Full HD)
3. **Lens**:3.5-8.5mmvarifocallens

Video Performance:

1. **Frame Rate**:30fpsatfullresolution
2. **Compression**:H.264,H.265,andMJPEGformats
3. **Night Vision**: Infrar edLED for low-light conditions

Connectivity:

1. **Network Inter face** :Ethernet(RJ-45)
2. **Wireless Capability**: Optional(Wi-Fi)
3. **Protocols**:IPv4, IPv6, HTTP,HTTPS, RTSP, and ONVIF compatible

Storage:

1. **Local Storage**: Micro SD cards lot(supports up to 128GB)
2. **Remote Storage**: Compatible with NVR (Network Video Recorder)

Features:

1. **Motion Detection**: Customizable sensitivity and detection areas
2. **Alerts** :Email notifications and push alerts for suspicious activity
3. **User Access Control**: Multi-level user authentication for secure access

Power Supply:

1. **Power Source** :PoE (Power over Ethernet) or DC power supply

Risk

- **Privacy Concerns**: CCTV may infringe on the privacy of employees, especially if cameras are placed in sensitive areas.

- **Data Securit yRisks** :Video footage can be vulnerable to hacking or unauthorized access, potentially exposing sensitive information.

- **System Malfunctions**: Cameras can fail due to technical issues, leading to gaps in surveillance and security.

Mitigation

Privacy Concerns:

- Clearly define areas where cameras will be installed to avoid monitoring private spaces (e.g., restrooms, break rooms).
- Inform employees about the presence of CCTV and the purpose of surveillance to foster transparency.

Data Security Risks:

- Implement strong passwords and encryption for accessing CCTV footage.
- Regularly update software and firmware to protect against vulnerabilities.

System Malfunctions:

- Schedule regular maintenance and inspections to ensure all cameras and equipment are functioning correctly.
- Install backup systems or redundant cameras to cover critical areas.

Vulnerabilities

Unauthorized Access:

- CCTV systems can be susceptible to unauthorized access if passwords are weak or not regularly updated ,allowing intruders to view live feeds or recorded footage.

Network Vulnerabilities:

- If the CCTV system is connected to a network, it may be exposed to cyber threats such as hacking, malware, or denial-of-service attacks ,compromising the entire system.

Insufficient Encryption:

- Lack of proper encryption for videofeeds and stored footage can make sensitive data susceptible to interception during transmission or unauthorizedaccess.

Policy:

Access Control:

- Access to live feed sand recorded footage will be restricted to authorized personnel only. Strong passwords and multi-factor authentication will be implemented to protect access.

Data Protection:

- All video footage must be stored securely ,with encryption applied to both in-transit and at-rest data, in compliance with **GDPR** (General Data Protection Regulation) and other relevant data protection laws.

REFERNCE: ISO/IEC19795-1:2006,ISO/IEC29100:2011