SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

M.SC. COMPUTER SCIENCE

PONDICHERRY UNIVERSITY

NAME : Harshitha Nakirekanti

REGISTER NO : 23370039

SEMESTER : 3nd SEMESTER

SUBJECT : International security system

ASSINGMENT : IT Assets Management

S.no	Asset
1	PERSONAL COMPUTER
2	BIO MATRIC SCANNER
3	UPS(Numeric Digital 1000 Plus-V)
4	CISCO WIRELESS ACCESS POINT
5	HDMI CABLE
6	PRINTER (CANON)
7	CCTV (Closed-Circuit Television)
8	PATCH CABLE
9	PROJECTER
10	NEW SMART BOARD LINE

1.PERSONAL COMPUTER

ABOUT:

Personal computer assets in a lab typically include desktops, monitors, and peripherals like keyboards and mice. These are essential for running experiments, processing data, and supporting lab workflows.

Ownership details:

Location status: Computer lab (ground floor) department of computer science

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department)

Users: students ,staff, professors.

SPECIFICATION :

Hardware Specifications

- Device Name: DCS217
- Model: HP 280 G4 MT Business PC
- Processor: Intel(R) Core(TM) i5-8500 CPU @ 3.00 GHz
- Installed RAM: 8.00 GB (7.83 GB usable)
- System Type: 64-bit operating system, x64-based processor
- Pen and Touch: No pen or touch input available

Software Specifications

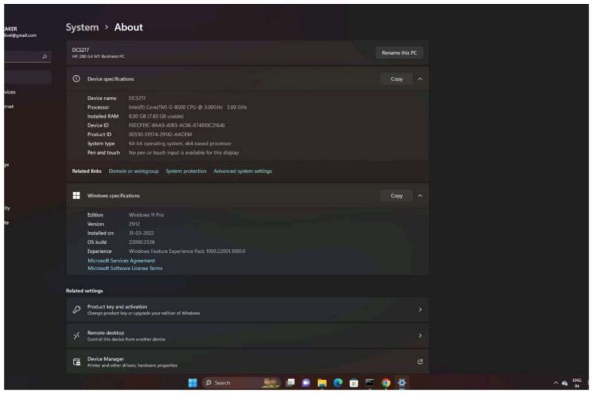
- Operating System Edition: Windows 11 Pro

- Version: 21H2
- Installed On: 25-05-2022
- OS Build: 22000.2538
- Experience: Windows Feature Experience Pack 1000.22000.1000.0-

Network information:

Ethernet Adapter Ethernet 1

- Description: Realtek PCIe GbE Family Controller
- Physical Address (MAC): C4-65-16-21-C2-4A



- IPv4 Address: 10.10.32.170 (Preferred)
- Subnet Mask: 255.255.254.0
- Default Gateway: 10.10.32.1
- DNS Servers: 8.8.8.8, 14.139.5.5 , 4.2.2.2

Ethernet Adapter Ethernet 2 (VirtualBox Host-Only)

- Description: VirtualBox Host-Only Ethernet Adapter
- Physical Address (MAC): 0A-00-27-00-00-10
- IPv4 Address: 192.168.56.1 (Preferred)
- Subnet Mask: 255.255.255.0

Wireless LAN Adapter Wi-Fi

- Description: Realtek RTL8821CE 802.11ac PCIe Adapter
- Physical Address (MAC)**: A4-FC-77-24-8E-13
- Media State: Disconnected

RISK

Data Loss: Accidental deletion, hardware failure.

Cyber Threats: Malware, ransomware.

Physical Damage: Mishandling, power surges.

VULNERABILITIES

Weak Authentication: Poor passwords, no multi-factor.

Outdated Systems: Unpatched software.

Lack of Protection: No firewalls, unsecured Wi-Fi

MITIGATION

Cybersecurity: Strong passwords, antivirus, updates.

Environmental: Efficient PC use, e-waste management.

Financial: Data encryption, restricted access.

REFERNCE:

- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations

2.BIO MATRIC SCANNER

ABOUT:

Biometric scanners in laboratories are advanced devices that identify individuals through unique biological traits, such as fingerprints, 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.

Ownership details:

Location status: Entrance of LH (department of computer science)

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:** Mangement,staff,teachers.

Purpose: Used to monitor real time activity.

SPECIFICATION:

Hardware :

- **Model**: XYZ-500
- **Processor**: Dual-Core ARM Cortex A7
- **Memory**: 512MB RAM, 4GB Flash Memory
- **Display**: 3.5-inch TFT LCD, 320x240 pixels
- **Biometric Sensor**: Optical fingerprint sensor, 500 DPI, stores up to 10,000 templates
- **Card Reader**: RFID/MIFARE/EM, up to 10,000 card templates
- **Network**: Ethernet (10/100 Mbps), optional Wi-Fi (2.4 GHz)
- **Interfaces**: USB 2.0, RS232/RS485
- **Power**: DC 12V/1.5A, 2000mAh battery backup

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°C to 50°C, 20%-80% humidity
- **Certifications**: CE, FCC, RoHS

RISKS

- **Data Breaches**: Unauthorized access to biometric data can result in identity theft.
- **Spoofing Attacks**: Biometric systems can be deceived by fake fingerprints, masks, or recordings.
- **Privacy Concerns**: Storing and collecting biometric data raises privacy issues.

VULNERABILITIES

- **Insecure Storage**: Lack of encryption may expose biometric data.
- **Limited Authentication**: Single-factor biometric systems (e.g., only fingerprints) can be less secure.

MITIGATION STRATEGIES

- **Encryption**: Encrypt biometric data both at rest and in transit.
- **Multi-Factor Authentication**: Combine biometrics with other methods like passwords or tokens for added security.
- **Regular Audits**: Conduct periodic security audits and vulnerability assessments on biometric systems.

POLICIES

- **Data Protection Policy**: Set clear guidelines on how biometric data is collected, stored, and shared.
- **Access Control Policy**: Define who can access biometric systems and data, ensuring only authorized personnel have access.

REFERNCE: ISO/IEC 19795-1:2006,ISO/IEC 29100:2011

3.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 features typically

include a sealed lead-acid battery, input and output ports, and cooling vents.

Ownership details:

Location status: Computer lab (ground floor) department of computer science

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department)

Users: students ,staff, professors.

SPECIFICATION:

Hardware Specifications

1. **Power Capacity**: 1000 VA / 600W, suitable for supporting multiple devices like computers, routers, and small servers.
2. **Battery Type**: Sealed lead-acid battery, designed for long life and high reliability, with typically a 5–10 minute backup duration for moderate loads.
3. **Automatic Voltage Regulation (AVR)**: Stabilizes incoming 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**: Ventilation slots to prevent overheating, 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 or serial connectivity for connecting the UPS 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 onboard controls may enable periodic self-tests to ensure battery health and overall UPS functionality.

Risks

- **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.

Vulnerabilities

- **Aging Equipment:** Older UPS systems may be more prone to failures.
- **Physical Access:** Unauthorized physical access to the UPS can lead to tampering or sabotage.
- **Firmware Issues:** Outdated firmware can expose the system to security

Mitigation Strategies

- **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.

Policies

- **UPS Usage Policy:** Define guidelines for the appropriate use of UPS systems, i
- **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.

REFERNCE:

- ·ISO/IEC 19795-1:2006, focusing on standardized performance testing and operation.

4. CISCO WIRELESS ACCESS POINT

ABOUT:

Cisco wireless access point installed alongside a lighting fixture, likely

providing network coverage within an indoor environment. Such configurations are essential for ensuring comprehensive wireless network connectivity in spaces like offices, schools, or other facilities. The integration of wired and wireless infrastructure within a shared physical space reflects the effort to maintain network accessibility and support a variety of internet-enabled devices.

Ownership details:

Location status: Near room 318 (2nd floor) department of computer science

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:** students ,staff, professors.

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 nearby; might cause minor interference.

Software

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

RISKS

- **Unauthorized Access**: Intruders can enter the network via unsecured or misconfigured WAPs.
- **Data Interception**: Sensitive data is at risk without strong encryption.
- **Firmware Vulnerabilities**: Outdated firmware exposes the network to exploits.

VULNERABILITIES

- **Outdated Firmware**: Higher risk of known exploits.
- **Weak or No Encryption**: Inadequate encryption makes data vulnerable.
- **Default Configurations**: Default SSIDs and passwords create security weaknesses.

MITIGATIONS

- **Strong Authentication**: Use WPA3 and restrict access with MAC filtering or enterprise authentication.
- **Encryption**: Apply WPA3 or stronger encryption for data protection.
- **Firmware Updates**: Regularly update firmware to close security gaps.

REFERNCE:

- **ISO/IEC 19795-1:2006**: Aligning with standardized performance testing and security validation.

REFERNCE:

- **ISO/IEC 19795-1:2006**: Aligning with standardized performance testing and security validation.

5. 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 in 2002 and has since evolved with various versions that offer increasingly advanced features.

Ownership details:

Location status: Room no 318 (2nd floor) department of computer science
Owner: Pondicherry university (Department of computer science)
Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:** students ,staff, professors.
Purpose: Used to connect to moniter

SPECIFICATION:

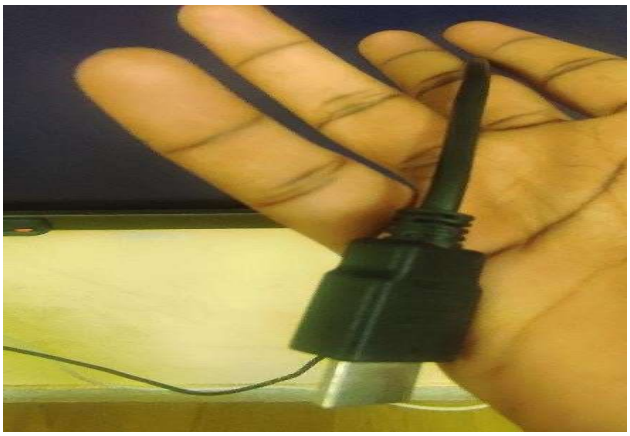
- **Resolution**: Up to 10K @ 120Hz (HDMI 2.1).
- · **Bandwidth**: 48 Gbps max (HDMI 2.1).
- **Audio**: Supports Dolby TrueHD, DTS-HD, and up to 32 audio channels (eARC for higher fidelity).
- · **HDR Support**: HDR10, Dolby Vision, HDR10+.
- · **VRR (Variable Refresh Rate)**: Reduces screen tearing, ideal for gaming.

- · **Cable Types**:

  - *Standard*: Up to 1080p.
  - *High-Speed*: Up to 4K @ 30Hz.
  - *Premium High-Speed*: 4K @ 60Hz with HDR.
  - *Ultra High-Speed*: 4K @ 120Hz, 8K @ 60Hz, required for HDMI

2.1.

- **Compatibility**: Backward compatible with older HDMI versions.



RISKS

1. **Data Breaches**: Unauthorized access may lead to loss or theft of sensitive data.
2. **System Failures**: Hardware or software issues that disrupt operations.
3. **Phishing Attacks**: Attempts to trick employees into revealing confidential info.

MITIGATIONS

1. **Encryption**: Secures data by making it accessible only to authorized users.
2. **Access Control**: Restricts access based on user roles to protect sensitive info.
3. **Regular Security Audits**: Routine checks to detect and fix vulnerabilities.

VULNERABILITIES

1. **Outdated Software**: Missing security patches, increasing exploitation risk.
2. **Weak Passwords**: Higher chance of unauthorized access.
3. **Unsecured Networks**: Data is vulnerable to interception on unprotected connections.

6.PRINTER (CANON)

ABOUT:

The Canon imageRUNNER 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 straightforward control with Canon's quality imaging technology, allowing users to handle typical document workflows effectively

Ownership details:

Location status: Office room (1st floor department of computer science)

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:**

Mangement,staff,teachers.

Purpose: Used to monitor real time activity.

Specifications:

Functionality:

1. Copying: High-resolution document reproduction.
2. Printing: Support for monochrome printing.
3. ***Scanning*****:** Basic scan functions for archiving or digital transfer.

Paper Handling:

1. Supports a variety of paper sizes and types.
2. Has an automatic document 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 for non-technical users.

FEATURES:

- **Multi-Functionality**: Capable of copying, printing, and basic scanning, making it a versatile choice for everyday office tasks.
- **User-Friendly Interface**: Simple control panel with an LCD screen and physical buttons, allowing easy access to core functions for users with minimal technical skills.

RISKS

- **Security Risks**: Printers can be hacked, leading to data breaches.
- **Compatibility Issues**: May not be compatible with all operating systems or software.
- **High Supply Costs**: Ink and toner can be expensive.

VULNERABILITIES

- **Security**: Lack of strong passwords, outdated firmware, and misconfigured security settings can allow unauthorized access.
- **Compatibility**: Compatibility issues with operating systems and software if drivers aren't updated.

MITIGATION STRATEGIES

- **Enhance Security**:
  - Use strong, unique passwords for networked printers.
  - Enable firewalls and disable unused services for added security.
- **Check Compatibility**:
  - Verify printer compatibility with operating systems and software before purchasing.

POLICIES

- **Security Policy**:
  - Require strong passwords and keep firmware up to date. ○ Set up firewalls and disable unnecessary features for networked printers.

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 within 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.

7.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.

Ownership details:

Location status: Room no 318 (2nd floor) department of computer science

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:**

Admin.

Purpose: Used to monitor real time activity.

Specifications:

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

Camera Type:

1. **Type**: IP Camera
2. **Resolution**: 1920 x 1080 (Full HD)
3. **Lens**: 3.5-8.5 mm varifocal lens

Video Performance:

1. **Frame Rate**: 30 fps at full resolution
2. **Compression**: H.264, H.265, and MJPEG formats
3. **Night Vision**: Infrared LED for low-light conditions

Connectivity:

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

Storage:

1. **Local Storage**: MicroSD card slot (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

RISKS

- **Privacy Concerns**: CCTV may infringe on employee privacy, especially in sensitive areas.
- **Data Security Risks**: Video footage is vulnerable to hacking or unauthorized access.
- **System Malfunctions**: Technical issues may cause camera failures, leading to surveillance

VULNERABILITIES

- **Unauthorized Access**: Weak or outdated passwords can allow intruders to access live feeds or recordings.
- **Network Vulnerabilities**: Connected CCTV systems may be exposed to hacking, malware, or denial-of-service attacks.
- **Insufficient Encryption**: Lack of encryption for video feeds and stored footage increases the risk of interception or unauthorized access.

MITIGATIONS

- **Privacy Concerns**: ○ Install cameras only in designated, non-private areas.
  - Inform employees about CCTV locations and purposes to ensure transparency.
- **Data Security Risks**:
  - Use strong passwords and encryption for accessing footage. ○ Regularly update software and firmware to prevent security breaches.

Policy:

Access Control:

- Access to live feeds and 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/IEC 19795-1:2006,ISO/IEC 29100:2011

8.PATCH CABLE

ABOUT:

The patch cable in the lab is essential for network connectivity but is vulnerable to wear, environmental damage, and security risks. Regular inspections, proper cable management, and secure connections mitigate these risks. Including the cable in an asset inventory ensures effective tracking and maintenance.

Ownership details:

Location status: Room no 318 (2nd floor) department of computer science

Owner: Pondicherry university (Department of computer science)

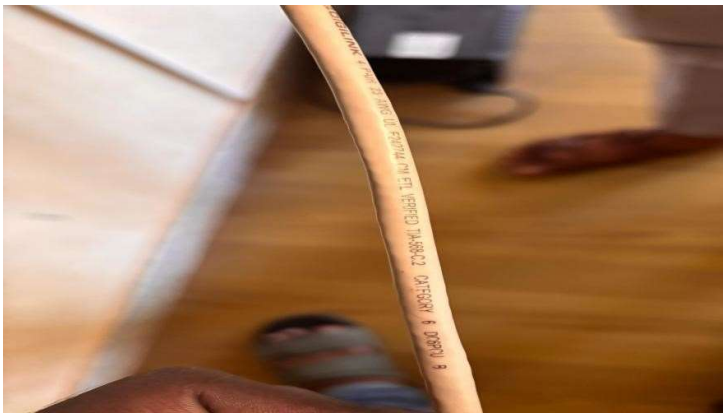
Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:** students ,staff, professors.

Purpose: Used to connect to internet

SPECIFICATION:

- Brand: DigiLink
- Type: Ethernet Patch Cable
- Configuration: 4 Pair
- Gauge: 23 AWG (American Wire Gauge)
- Standard Compliance: UL E247344 CM (Communication Cable Standard)
- Certification: ETL Verified
- Category: Category 6 (CAT6)
- Standard: TIA-568-C.2

- Sheath Material: Likely PVC or a similar material, though not specified in the image



RISK

- **Connection Failure**: Patch cables are prone to wear, leading to network disruptions.
- **Data Interception**: Unsecured or damaged cables may expose data to unauthorized access.
- **Physical Damage**: Patch cables can be damaged by foot traffic, spills, or misplacement, affecting functionality.

VULNERABILITIES

- **Cable Wear**: Repeated plugging/unplugging or poor handling degrades cable quality.
- **Unsecured Connections**: Poorly secured cables can cause network disruptions.
- **Environmental Exposure**: Extreme temperatures, moisture, or chemicals can damage cables

MITIGATION STRATEGIES

- **Regular Inspection**: Periodically check cables for wear and replace if needed.
- **Proper Cable Management**: Use cable management practices to prevent tangling and damage.
- **Environmental Protection**: Use covers or conduits to shield cables from environmental hazards.

ASSET MANAGEMENT POLICY

- **Inventory Management**: Label and record each cable's type, length, location, and purchase date in inventory.
- **Maintenance Schedule**: Include cables in regular audits and maintenance schedules to ensure functionality.

REFERNCE:

- ISO 55001:2014,
- ISO/IEC 27001:2013
- ISO 55001:2014,

9.PROJECTOR

ABOUT:

The projector serves as an essential tool for presentations, collaborative work, and educational sessions within the lab environment. Effective management of this asset ensures its reliability, security, and optimal performance, thereby supporting the lab's operational needs. Key components of the asset management plan

include identifying risks (such as data security and hardware malfunction).

Ownership details:

Location status: Computer lab (ground floor) department of computer science

Owner: Pondicherry university (Department of computer science)

Incharge: Dr. S. K. V. Jayakumar (Head of department), **Users:** students ,staff, professors.

SPECIFICATION:

Brand: Epson ·

Model: EB-X41

INPUTS:

- HDMI
- USB-A
- USB-B
- Audio
- Video
- Computer (likely VGA)

Lamp Type: ELPLP96 ·

Features:

- Status Indicator
- Lamp and Temperature Indicators

- Control Buttons: Power, Source Search, Menu, Esc, Volume, and Navigation buttons

· warrrenty:

Out of warrenty

RISK

- **Image Quality Degradation**: Dust on the lens or internal components reduces image clarity.
- **Overheating**: Prolonged use without ventilation can cause overheating, damaging components.

ULNERABILITIES

- **Physical Damage**: Projector lens or housing may be damaged by falls, knocks, or mishandling.
- **Unsecured Access**: Network-connected projectors are vulnerable to unauthorized access.
- **Firmware Vulnerabilities**: Outdated firmware increases security risks.

ULNERABILITIES

- **Physical Damage**: Projector lens or housing may be damaged by falls, knocks, or mishandling.
- **Unsecured Access**: Network-connected projectors are vulnerable to unauthorized access.
- **Firmware Vulnerabilities**: Outdated firmware increases security risks, especially on networked projectors.

10.NEW SMARTLINE BOARD

ABOUT:

The Newline Smart Board is an advanced interactive display designed to enhance collaborative work spaces, educational environments, and remote communication. It features a user-friendly touchscreen interface with 4K Ultra HD resolution, making content and visuals highly engaging. With built-in Android or Windows options, it supports a wide range of applications and software, enabling seamless integration across various operating systems.

Ownership details:

Location status: seminar hall (ground floor) departmentof computerscience
Owner: Pondicherry university (Departmentof computerscience)
Incharge: Dr. S. K. V. Javakumar (Head of department)
Users: students,staff, professors.

SPECIFICATIONS:

Hardware Specifications:

- **Device**: Newline Smart Board
- **Display Resolution**: Likely 4K Ultra HD (common for Newline 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.

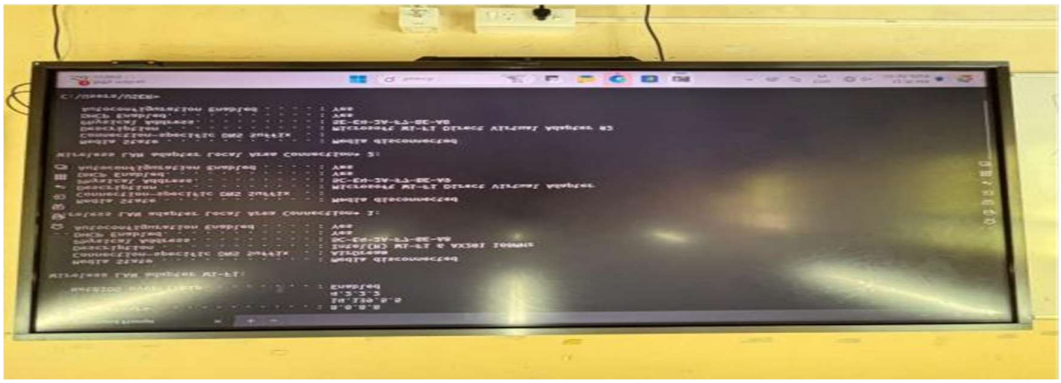
Network Information:

- **DNS Servers**:

- Primary: 8.8.8.8 (Google Public DNS) ○ Secondary: 14.139.5.5 (local or custom DNS) ○ Tertiary: 4.2.2.2 (Level 3 DNS)

- **Wi-Fi Adapter**: Intel(R) Wi-Fi 6 AX201 160MHz
  - **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)**:
    - Adapter 1: 5C-E4-2A-F7-BE-A9
    - Adapter 2: 5E-E4-2A-F7-BE-A8
  - **DHCP**: Enabled
  - **Auto-configuration**: Enabled



VULNERABILITIES:

- **Unauthorized Access**: Risk of unauthorized users accessing settings or data.
- **Malware Attacks**: Window OS environment vulnerable to malware
- **Malware Infection**: Windows-based OPS modules may be susceptible to malware,risking network security.

RISK:

- **Unauthorized Access**: Unauthorized access to smart board settings or data, leading to breaches or misuse.
- **Malware Infection**: Windows-based OPS modules may be susceptible to malware, risking network security.

MITIGATION STRATEGEIS:

- **Regular Updates:** Enable automatic OS and app updates.
- **Access control**:use password protection and user roles to restrict access.
- **Network Security:** Apply WPA3 encryption and VPNs for secure connections.

REFERENCE:

- **ISO 55001**: This specifies requirements for an asset management system, helping organizations effectively manage their assets throughout their lifecycle.
- **ISO 55000**: This standard provides an overview of asset management and outlines the principles and terminology.