PONDICHERRY UNIVERSITY

(A CENTRAL UNIVERSITY)

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

M.SC. COMPUTER SCIENCE

PONDICHERRY UNIVERSITY

NAME	:	TEENA SEBASTIAN
REGISTER NO	:	23370066
SEMESTER	:	3nd SEMESTER
SUBJECT	:	ISM (IT Asset management assignment)

S.no	Asset
1	COMPUTERS (DESKTOP/LAPTOP)
2	NETWORK SWITCHES
3	SERVERS
4	PRINTER AND SCANNER
5	PROJECTOR
6	UPS
7	SOFTWARE APPLICATIONS
8	DATA STORAGE DEVICES(USB,SSD)
9	FIREWALL
10	SMART BOARD

1. **COMPUTERS**(DESKTOPS/LAPTOPS)

ROLE:

- Serve as the primary workstations for students and staff.
- Enable users to run various software applications for tasks such as word processing, programming, graphic design, and research.
- Facilitate access to the internet for research, online learning platforms, and collaboration tools.
- Support educational programs through interactive software and multimedia presentations.

RISKS :

- **Hardware Failure:** Can result from wear and tear, leading to data loss and downtime.
- **Malware Infection:** Can compromise sensitive data and system integrity.
- **Unauthorized Access:** Risks from weak passwords or unregulated access.

MITIGATION PLAN:

- **Regular Maintenance:** Schedule routine checks and hardware upgrades.
- **Antivirus Software:** Install and update reputable antivirus software regularly.
- **Access Controls:** Implement strong password policies and multi-factor authentication.

2. NETWORK SWITCHES

ROLE:

- Act as the central point for connecting multiple devices within a local area network (LAN).
- Manage data traffic efficiently, ensuring that packets are directed to the correct devices without unnecessary delays.
- Enable communication between computers, servers, printers, and other networked devices.
- Help maintain network performance by preventing collisions and managing bandwidth effectively.

RISKS :

- **Network Congestion:** Can slow down communication between devices.
- **Unauthorized Access:** Vulnerabilities may allow unauthorized users to connect.
- **Physical Damage:** Risk from spills, falls, or other environmental factors.

MITIGATION PLAN:

- **Performance Monitoring:** Use network monitoring tools to identify congestion.
- **Physical Security:** Secure switches in locked cabinets and restrict access.
- **Regular Inspections:** Conduct routine checks for physical damage.

3. SERVERS

ROLE:

- Function as centralized resources that host applications, databases, and files used by the computer lab.
- Provide services such as file storage, printing, email, and database management, enabling collaborative work among users.
- Manage user accounts and permissions, ensuring secure access to resources.
- Enable virtual learning environments, hosting e-learning platforms and educational software.

RISKS :

- **Data Breaches:** Compromise of sensitive information due to security flaws.
- **System Failures:** Downtime can disrupt services and impact users.
- **Overheating:** Can lead to hardware damage or failure.

MITIGATION PLAN:

- **Regular Backups:** Implement automated backup solutions for critical data.
- **Firewalls and IDS:** Use firewalls and intrusion detection systems to protect servers.
- **Cooling Solutions:** Ensure adequate cooling systems and monitor temperatures.

4. PRINTER AND SCANNER

ROLE:

- Offer physical output for digital documents, allowing students to print assignments, reports, and study materials.
- Provide scanning capabilities for converting physical documents into digital formats, facilitating easy sharing and storage.
- Support administrative tasks by enabling the printing of forms, flyers, and other materials needed in the lab or school environment.

RISKS :

- **Data Leaks:** Sensitive documents can be left unprotected.
- **Unauthorized Access:** Poor access controls can lead to misuse.
- **Hardware Malfunction:** Can disrupt printing/scanning capabilities.

□

MITIGATION PLAN:

- **Secure Print Options:** Use features like PIN codes for printing sensitive documents.
- **Access Control:** Limit printer and scanner access to authorized users.
- **Regular Maintenance:** Schedule periodic checks to ensure functionality

5. PROJECTOR

ROLE:

- Facilitate group learning by displaying presentations, videos, and other educational materials to larger audiences.
- Enhance lectures and demonstrations, making information more accessible and engaging.
- Support interactive learning experiences by allowing real-time feedback and collaboration during presentations.

RISKS :

- **Hardware Failure:** Can disrupt presentations and lessons.
- **Outdated Software:** May lead to compatibility issues or security vulnerabilities.
- **Unauthorized Access:** Risk of tampering with settings or inputs.

MITIGATION PLAN:

- **Maintenance Schedule:** Regularly clean and service projectors.
- **Firmware Updates:** Keep software updated to ensure security and functionality.
- **Access Controls**: Restrict access to projector settings and control interfaces.

6. UPS

ROLE:

- Provide backup power during electrical outages, preventing data loss and hardware damage.
- Protect sensitive equipment from power surges and fluctuations, ensuring stable operation.
- Allow for safe shutdown of computers and servers during power interruptions, safeguarding against abrupt disruptions.

RISKS :

- **Power Outages:** Sudden loss of power can lead to data loss.
- **Battery Failure:** Old batteries may fail unexpectedly.
- **Overheating:** Can damage equipment connected to the UPS

MITIGATION PLAN:

- Regular Testing: Conduct routine tests of UPS systems and replace batteries as needed.
- Proper Ventilation: Ensure UPS units are in well-ventilated areas.
- Surge Protectors: Use additional surge protection for connected devices.

7. SOFTWARE APPLICATIONS

ROLE:

- Enable users to perform specific tasks tailored to educational needs, such as writing, programming, data analysis, and graphic design.
- Support collaborative projects through tools for communication, project management, and file sharing.
- Enhance learning experiences through educational software, simulations, and e-learning platforms.

RISKS :

- **Licensing Issues**: Using unlicensed software can lead to legal consequences.
- **Security Vulnerabilities**: Outdated software can be exploited by attackers.
- **Compatibility Problems**: New software may not work with existing systems.

MITIGATION PLAN:

- **Maintain Licenses:** Keep track of software licenses and renew them on time.
- **Regular Updates:** Apply updates and patches promptly to fix vulnerabilities.
- **Compatibility Testing:** Test new software in a controlled environment before deployment.

8. DATA STORAGE DEVICES

ROLE:

- Allow users to transfer, store, and back up data externally, enhancing data portability and accessibility.
- Enable students to save their work and carry it easily between school and home.
- Provide a solution for additional storage needs, especially for large files or projects.

RISKS :

- **Data Loss:** External drives can be damaged or lost, resulting in data loss.
- **Malware Transfer:** Infected USB drives can spread malware to other systems.
- **Unauthorized Access:** Sensitive data can be accessed if not properly secured.

MITIGATION PLAN:

- **Regular Backups:** Ensure data on external drives is backed up regularly.
- **Use Encryption:** Encrypt sensitive data stored on external devices.
- **Access Policies:** Restrict the use of removable storage devices to authorized personnel only.

9. FIREWALL

ROLE:

- Protect the network from unauthorized access and cyber threats by monitoring and controlling incoming and outgoing traffic.
- Implement security policies that dictate which types of traffic are allowed or blocked, helping to prevent malicious activities.
- Act as a barrier between the internal network and external sources, ensuring the integrity and confidentiality of sensitive data.

RISKS :

- **Configuration Errors:** Incorrect settings can expose the network to threats.
- **Vulnerabilities to Attacks:** Outdated firewalls may be exploited by attackers.
- **Hardware Failure:** Physical failures can result in a loss of protection.

MITIGATION PLAN:

- **Review Firewall Rules:** Regularly audit and update firewall configurations.
- **Apply Firmware Updates:** Keep firewall software current to address vulnerabilities.
- **Implement Redundancy:** Use redundant firewalls to maintain protection during failures.
- **Monitoring Tools:** Employ monitoring solutions to track traffic and identify threats promptly.

10. SMARTBOARD

ROLE:

- **Interactive Learning Tool:** Enhances lessons with digital content and interactive features.
- **Collaboration:** Allows multiple users to engage simultaneously.
- **Presentation:** Central point for displaying multimedia content.

RISKS :

- **Technical Failures:** Hardware or software issues can disrupt lessons.
- **Security Vulnerabilities:** Risk of unauthorized access to network-connected boards.
- **User Misuse:** Improper use by students may disrupt functionality.
- **Obsolescence:** Rapid tech advancements may render boards outdated.

MITIGATION PLAN:

- **Regular Maintenance:** Schedule checks and updates to prevent technical issues.
- **Network Security:** Use strong passwords and firewalls to protect access.
- **User Training:** Educate users on proper use to reduce misuse.
- **Upgrade Strategy:** Plan for regular assessments and upgrades to keep technology current.