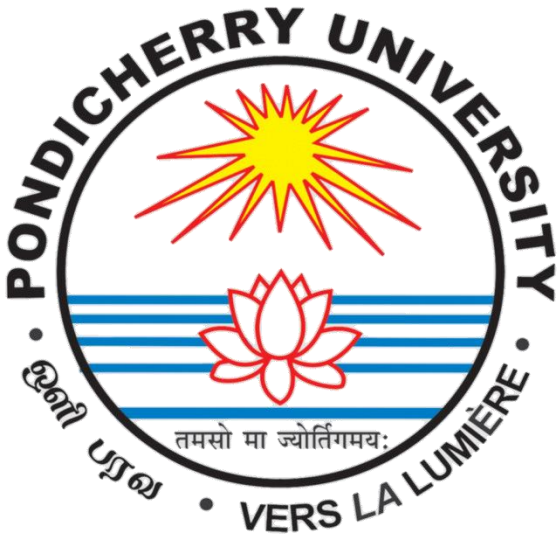
PONDICHERRY UNIVERSITY

(A Central University)



SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

M.Sc. Computer Science

NAME	:	MAHALAKSHMY R
REGISTER NO	:	23370083
SUBJECT	:	INFORMATION SECURITY MANAGEMENT
SUBJECT CODE	:	CSEL 446
SUBMISSION DATE	:	October 28,2024.

ASSETS IN IT Lab

1. Workstations (Desktops and Laptops)

Role: Workstations serve as the primary computing devices for students, researchers, and staff in a lab, enabling tasks such as data processing, internet access, and software development.

Risk: Workstations face risks such as unauthorized access, malware infections, and data breaches. Since they're shared or accessible by multiple users, the potential for accidental or intentional tampering, data leakage, and exposure to phishing attacks increases.

Owner: The IT Support Team generally manages workstation security, handling Asoftware updates, access control, and endpoint protection.

Mitigation: Installing endpoint security software with regular scanning and enforcing strict authentication mechanisms can protect against unauthorized access. Applying frequent software and OS updates and limiting user permissions to reduce adminisaccess helps prevent malware and tampering. Educating users on safe practices also mitigates phishing risks.

---

2. Network Routers and Switches

Role: Routers and switches ensure connectivity within the lab and to external networks, facilitating data transfer across devices and applications.

Risk: These devices are vulnerable to network attacks such as unauthorized access, eavesdropping, or Distributed Denial of Service (DDoS) attacks, which can compromise data integrity and network availability.

Owner: Network Administrators oversee configuration, monitoring, and updates of network devices.

Mitigation: Enforcing strong password policies, regularly updating firmware, and setting up firewalls to control incoming and outgoing traffic minimizes risk. Implementing network segmentation and using intrusion detection systems (IDS) also protects against internal and external threats.

---

3. Database Management System (DBMS)

Role: DBMS software handles storage, retrieval, and management of critical lab data, such as experimental results and user information.

Risk: DBMSs are vulnerable to SQL injection attacks, unauthorized access, and data corruption. Misconfigurations can also lead to data leakage or loss.

Owner: Database Administrators (DBAs) manage DBMS configuration, security, and access control.

Mitigation: Using parameterized queries and stored procedures reduces SQL injection risk, while implementing role-based access control (RBAC) limits data exposure. Encryption of stored data and regular database backups ensure data integrity and recoverability in case of incidents.

---

4. Virtual Machines (VMs)

Role: VMs are often used for testing, simulations, and isolated experiments, providing an efficient way to simulate various environments without needing physical hardware.

Risk: VMs can face hypervisor attacks, unauthorized access, and data leakage. Cross-VM data exposure is also a risk if VMs are not properly isolated.

Owner: The IT Virtualization Team typically manages VM security, ensuring they are isolated and regularly updated.

Mitigation: Applying secure hypervisor configurations, patching vulnerabilities, and enforcing isolation between VMs reduce the chance of cross-contamination. Configuring access control and conducting regular monitoring help detect unauthorized access attempts, and regular snapshots allow recovery in case of failures.

---

5. Network Attached Storage (NAS)

Role: NAS systems store shared files, making it easy for lab users to access shared resources, backups, and large datasets.

Risk: NAS devices are prone to unauthorized access, ransomware, and data loss, especially if they lack encryption and access restrictions.

Owner: The IT Department manages NAS devices, handling permissions, configuration, and backup routines.

Mitigation: Enforcing multi-factor authentication (MFA) and user-level access control ensures that only authorized users can access sensitive data. Encrypting stored data protects it in case of a breach, and regularly scheduled backups prevent data loss from accidental deletion or ransomware attacks.

---

6. Anti-Malware Software

Role: Anti-malware software is crucial for protecting all lab devices from viruses, spyware, ransomware, and other malicious threats.

Risk: Without regular updates, anti-malware software may fail to detect new threats, increasing vulnerability to infections.

Owner: The IT Security Team manages anti-malware deployment, ensuring it's updated and configured on all devices.

Mitigation: Enabling automatic updates for malware definitions, configuring real-time scanning, and conducting regular manual scans enhance security. Limiting software installation permissions also prevents the introduction of unverified software, reducing malware risks.

---

7. Firewalls

Role: Firewalls monitor and control incoming and outgoing network traffic, acting as a barrier between internal systems and external networks.

Risk: Firewalls can be susceptible to misconfiguration or outdated firmware, leaving the network open to attacks like data breaches or Denial of Service (DoS) attacks.

Owner: Network Security Team members are responsible for firewall configuration and maintenance.

Mitigation: Configuring strict access control rules and updating firewall firmware regularly can reduce vulnerabilities. Employing logging and monitoring tools for suspicious activity allows for quick response, and performing regular audits helps maintain effective security policies.

---

8. Access Control System

Role: Access control systems manage entry to secure lab areas, typically through badge readers, biometric scanners, or keypads, helping protect sensitive equipment and data.

Risk: These systems are vulnerable to unauthorized access attempts, tampering, and potential data privacy concerns if access logs are improperly handled.

Owner: Facilities Management, with IT Security's support, oversees access control systems.

Mitigation: Using multi-factor authentication (e.g., badge plus PIN) strengthens security. Regularly maintaining and updating the system prevents malfunctions, and ensuring access logs are encrypted protects privacy. Access should be restricted to authorized personnel, with logs regularly reviewed for suspicious activity.

---

9. Remote Desktop Software

Role: Remote desktop software allows users to access lab systems from remote locations, providing flexibility for offsite work.

Risk: If not secured, remote desktop software may permit unauthorized access, increasing the risk of data breaches and malware infections.

Owner: The IT Security Team manages access control and configuration for remote desktop software.

Mitigation: Implementing multi-factor authentication (MFA) for remote access and encrypting connections through Virtual Private Networks (VPNs) strengthens security. Limiting administrative access and regularly monitoring access logs helps detect unusual activity.

10. Environmental Control Systems (ECS)

Role: ECS (such as HVAC systems) regulate the environment, maintaining conditions optimal for lab equipment and experiments.

Risk: If compromised, ECS could be tampered with, causing damage to temperature-sensitive equipment or affecting the safety of experiments.

Owner: Facilities Management, with IT Security's support, oversees ECS, ensuring it functions within safety and security parameters.

Mitigation: Encrypting control data and configuring access restrictions prevent unauthorized modifications. Regular software updates reduce vulnerabilities, and setting up alerts for abnormal readings allows for quick response to environmental anomalies.

---

11. Data Backup and Recovery System

Role: Backup systems ensure that critical lab data can be restored in case of accidental deletion, system failure, or cyberattacks.

Risk: Backup systems can be vulnerable to unauthorized access, data corruption, and ransomware attacks, which could compromise or destroy data.

Owner: The IT Backup and Recovery Team manages data backups, ensuring they are performed regularly and securely stored.

Mitigation: Encrypting backups both at rest and in transit prevents unauthorized access. Isolating backups from the primary network helps protect them from ransomware attacks. Regularly testing the recovery process ensures backups are functional and up-to-date.

---

12. Patch Management Software

Role: Patch management software ensures that all lab systems and software remain up-to-date with security patches, reducing the risk of vulnerabilities.

Risk: Poor patch management can leave devices vulnerable to attacks exploiting outdated software. Missing patches create security gaps that attackers can leverage.

Owner: The IT Security Team is responsible for managing and automating patch processes for lab systems.

Mitigation: Configuring automatic patching for systems and enabling alerts for failed patches help ensure that security updates are consistently applied. Regularly auditing patch compliance helps identify and resolve any issues with patch installations.

---

13. Lab Management Software

Role: Lab management software coordinates scheduling, resource allocation, and equipment tracking, facilitating efficient use of lab resources.

Risk: If unprotected, lab management software can be vulnerable to data breaches, unauthorized access, and data tampering, affecting the scheduling and tracking of lab equipment.

Owner: Lab supervisors or designated IT personnel are responsible for configuring and securing lab management software.

Mitigation: Implementing role-based access control (RBAC), regular software updates, and encryption for sensitive data helps protect against

unauthorized access. Monitoring logs for unusual activity can help detect and respond to security incidents promptly.

---

14. Printers and Scanners

Role: Printers and scanners are often used for handling documents and experiment results, enabling hard-copy documentation and data digitization.

Risk: Shared printers and scanners can expose sensitive information if unauthorized individuals access printed or scanned data. Additionally, these devices are vulnerable to network-based attacks, such as eavesdropping on data in transit.

Owner: IT Support manages printer and scanner configuration, usage monitoring, and access control.

Mitigation: Implementing print job authentication (e.g., PIN-based release) restricts access to sensitive documents. Configuring printers to require network access credentials reduces unauthorized use, and encrypting data in transit ensures privacy. Regularly updating firmware protects against vulnerabilities.

---

15. CCTV and Security Cameras

Role: CCTV systems provide physical security for lab equipment, monitoring entry points and critical areas.

Risk: CCTV systems are vulnerable to unauthorized access, tampering, or footage exposure if not properly secured. Compromised video feeds may expose sensitive lab activities or equipment layout.

Owner: Facilities Management or the IT Security Team oversees CCTV operations, securing access and monitoring footage integrity.

Mitigation: Encrypting video feeds, using strong access control measures, and limiting access to footage protect against unauthorized viewing. Ensuring regular firmware updates reduces vulnerabilities, and maintaining activity logs allows for quick detection of access anomalies.