**PONDICHERRY UNIVERSITY**

**(A Central University)**



**SCHOOL OF ENGINEERING AND TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE**

**M.Sc. Computer Science**

NAME : R.NIVEDHA

REGISTER NO : 23370041

SUBJECT : INFORMATION SECURITY MANAGEMENT

SUBJECT CODE : CSEL 446

SUBMISSION DATE : October 28.2024.

|  |  |
| --- | --- |
| S.NO | ASSETS |
| 1 | PERSONAL COMPUTER |
| 2 | PROJECTOR |
| 3 | WIFI |
| 4 | CCTV |
| 5 | SMART BOARD |
| 6 | BIO METRIC |
| 7 | PRINTERS |
| 8 | NETWORKING CABLES |
| 9 | NETWORKING EQUIPMENT |

**PERSONAL COMPUTER**

**Personal Computer Specifications:**

1. Hardware:

- Processor (CPU): Intel Core i5/i7 or AMD Ryzen 5/7

- Memory (RAM): 8-16 GB

- Storage: 256-512 GB SSD or 1-2 TB HDD

- Graphics Card: Integrated or dedicated (NVIDIA/AMD)

- Display: 14-17 inches, Full HD/4K

2. Software:

- Operating System: Windows 10/11, macOS, or Linux

- Productivity Suite: Microsoft Office, Google Workspace

- Antivirus Software: Norton, McAfee, or Kaspersky

- Browser: Google Chrome, Mozilla Firefox

**Risks:**

1. Hardware Failure:

- Hard drive crash

- RAM failure

- CPU overheating

2. Software Vulnerabilities:

- Malware infections

- Phishing attacks

- Ransomware

3. Data Loss:

- Accidental deletion

- Thefts or losses

- Corruption

4. Security Threats:

- Hacking

- Spyware

- Adware

5. Physical Damage:

- Water damage

- Electrical surges

- Physical trauma

**Mitigation Strategies:**

Hardware:

1. Regular backups

2. Surge protectors

3. Dust cleaning

4. Cooling system maintenance

5. Hard drive encryption

Software:

1. Antivirus software updates

2. Firewall configuration

3. Strong passwords

4. Two-factor authentication

5. Regular software updates

Data Protection:

1. Cloud backups (Google Drive, Dropbox)

2. External hard drive backups

3. Data encryption (BitLocker, FileVault)

4. Secure file sharing

5. Regular data verification

Security:

1. Firewall configuration

2. Antivirus software

3. Strong passwords

4. Two-factor authentication

5. Regular security audits

Physical Protection:

1. Protective casing

2. Screen protectors

3. Water-resistant bags

4. Electrical surge protectors

5. Secure storage

**PROJECTOR**

Projector Specifications:

1. Display Technology:

- DLP (Digital Light Processing)

- LCD (Liquid Crystal Display)

- LCoS (Liquid Crystal on Silicon)

- LED (Light Emitting Diode)

2. Resolution:

- SVGA (800x600)

- XGA (1024x768)

- WXGA (1280x800)

- HD (1920x1080)

- 4K (3840x2160)

3. Brightness:

- Lumens (1000-5000)

4. Contrast Ratio:

- 1000:1 to 100,000:1

5. Connectivity:

- HDMI

- USB

- VGA

- Wireless (Wi-Fi, Bluetooth)

6. Lamp Life:

- 2000-5000 hours

7. Noise Level:

- 20-40 dB

Risks:

1. Hardware Failure:

- Lamp failure

- Power supply issues

- Cooling system malfunction

2. Image Quality Issues:

- Distorted images

- Color inaccuracies

- Low brightness

3. Connectivity Problems:

- HDMI port damage

- Wireless connectivity issues

4. Security Risks:

- Unauthorized access

- Data theft

5. Maintenance Risks:

- Dust accumulation

- Filter cleaning

- Software updates

Mitigation Strategies:

Hardware:

1. Regular lamp replacement

2. Power supply protection (surge protectors)

3. Cooling system maintenance

4. Dust cleaning

5. Filter replacement

Image Quality:

1. Regular calibration

2. Image adjustment

3. Focus adjustment

4. Color correction

Connectivity:

1. Secure HDMI connections

2. Wireless encryption (WPA2)

3. Regular software updates

4. Network configuration

Security:

1. Password protection

2. Access control

3. Data encryption

4. Regular security audits

WIFI

NETGEAR 6 WIFI

NETGEAR WiFi 6 Specifications

1. Technology Standards:

- Based on IEEE 802.11ax (WiFi 6)

- Enhanced data rates (up to 9.6 Gbps)

- Improved efficiency with OFDMA (Orthogonal Frequency Division Multiple Access)

\*\*2. Frequency Bands:\*\*

- Dual-band: 2.4 GHz and 5 GHz

- Supports both bands simultaneously for optimal performance

\*\*3. MU-MIMO:\*\*

- Multi-User, Multiple Input, Multiple Output technology

- Allows multiple devices to communicate simultaneously, reducing latency

\*\*4. Beamforming:\*\*

- Focuses signal directly to devices rather than broadcasting in all directions, improving range and performance

\*\*5. Security:\*\*

- Supports WPA3 encryption for enhanced security

\*\*6. Compatibility:\*\*

- Backward compatible with previous WiFi standards (802.11a/b/g/n/ac)

**### Risks**

\*\*1. Security Vulnerabilities:\*\*

- Potential for unauthorized access if security settings are not properly configured.

- Risk of exploitation of vulnerabilities in firmware or software.

\*\*2. Interference:\*\*

- Increased number of devices can lead to congestion and interference, especially in dense environments.

\*\*3. Hardware Limitations:\*\*

- Older devices may not fully utilize the capabilities of WiFi 6, leading to performance bottlenecks.

\*\*4. Adoption Barriers:\*\*

- Not all devices are compatible with WiFi 6, limiting the benefits for users with older technology.

**### Mitigation Strategies**

\*\*1. Strong Security Practices:\*\*

- Use WPA3 encryption and regularly update firmware to patch vulnerabilities.

- Change default passwords and configure a strong, unique passphrase.

\*\*2. Network Management:\*\*

- Utilize QoS (Quality of Service) settings to prioritize bandwidth for critical applications.

- Regularly monitor network performance and adjust settings to reduce congestion.

\*\*3. Device Upgrades:\*\*

- Encourage users to upgrade older devices to ensure compatibility and improved performance.

- Provide guidance on selecting WiFi 6-compatible devices.

\*\*4. Education and Awareness:\*\*

- Educate users about the benefits of WiFi 6 and best practices for network security.

- Share tips on minimizing interference, such as optimal placement of routers.

**CCTV**

CCTV Specifications:

1. Camera Type:

- Analog

- IP (Internet Protocol)

- HD (High Definition)

- 4K

2. Resolution:

- 720p

- 1080p

- 2MP

- 4MP

3. Lens Type:

- Fixed

- Varifocal

- Zoom

4. Field of View:

- Wide-angle

- Narrow-angle

5. Night Vision:

- Infrared (IR)

- Starlight

6. Connectivity:

- Wired (RJ45)

- Wireless (Wi-Fi)

7. Power:

- 12V DC

- PoE (Power over Ethernet)

8. Storage:

- DVR (Digital Video Recorder)

- NVR (Network Video Recorder)

- Cloud storage

**Risks:**

1. Security Breaches:

- Unauthorized access

- Hacking

2. Data Loss:

- Storage failure

- Data corruption

3. Image Quality Issues:

- Distortion

- Blur

4. Camera Tampering:

- Vandalism

- Theft

5. Power Outages:

- System downtime

- Data loss

6. Weather Conditions:

- Extreme temperatures

- Moisture

7. Maintenance Risks:

- Dust accumulation

- Lens damage

**Mitigation Strategies:**

Security:

1. Password protection

2. Access control

3. Encryption

4. Regular software updates

5. Secure network configuration

Data Protection:

1. Redundant storage

2. Backup systems

3. Data encryption

4. Secure data transfer

Image Quality:

1. Regular camera cleaning

2. Focus adjustment

3. Image optimization

4. Lens replacement

Camera Protection:

1. Tamper-proof housing

2. Vandal-resistant cameras

3. Regular inspections

4. Secure mounting

**Power Protection:**

1. UPS (Uninterruptible Power Supply)

2. Redundant power sources

3. Power conditioning

4. Regular maintenance

Weather Protection:

1. Weather-resistant housing

2. Temperature control

3. Humidity control

4. Regular inspections

Maintenance:

1. Regular cleaning

2. Software updates

3. Firmware updates

4. Hardware replacement

Best Practices:

1. Regular monitoring

2. Secure storage

3. User training

4. Compliance with regulations

5. Regular system audits

Here's a comprehensive overview of the specifications, risks, and mitigation strategies for each device:

CCTV:

Specifications:

- Resolution: 720p to 4K

- Field of View: Wide-angle to narrow-angle

- Night Vision: Infrared (IR) or Starlight

- Connectivity: Wired (RJ45) or Wireless (Wi-Fi)

- Storage: DVR/NVR or Cloud storage

Risks:

- Security breaches

- Data loss

- Image quality issues

- Camera tampering

- Power outages

Mitigation:

- Secure network configuration

- Regular software updates

- Password protection

- Redundant storage

- Tamper-proof housing

**Smart Board:**

Specifications:

- Display size: 50-100 inches

- Resolution: Full HD to 4K

- Touchscreen: Capacitive or Resistive

- Connectivity: HDMI, USB, Wi-Fi

- Operating System: Android or Windows

Risks:

- Data breaches

- Malware infections

- Unauthorized access

- Screen damage

- Connectivity issues

Mitigation:

- Secure network configuration

- Regular software updates

- Password protection

- Screen protection

- Limited user access

Biometric Devices:

Specifications:

- Fingerprint recognition

- Facial recognition

- Iris scanning

- Connectivity: USB, Wi-Fi

- Storage: Local or Cloud

Risks:

- Data breaches

- Identity theft

- False positives/negatives

- Device tampering

- Power outages

Mitigation:

- Secure network configuration

- Encryption

- Regular software updates

- Password protection

- Tamper-proof housing

Printers:

Specifications:

- Print resolution: 300-1200 dpi

- Print speed: 10-50 ppm

- Connectivity: USB, Wi-Fi, Ethernet

- Paper capacity: 100-500 sheets

Risks:

- Data breaches

- Print quality issues

- Paper jams

- Toner cartridge theft

- Maintenance costs

Mitigation:

- Secure network configuration

- Regular firmware updates

- Password protection

- Paper tray security

- Regular maintenance

Networking Cables:

Specifications:

- Category: Cat5e, Cat6, Cat7

- Length: 1-100 meters

- Speed: 1-10 Gbps

- Connectivity: RJ45

Risks:

- Signal degradation

- Interference

- Physical damage

- Data breaches

- Cable management

Mitigation:

- Regular cable testing

- Cable management systems

- Secure connections

- Cable protection

- Regular replacement

Networking Equipment:

Specifications:

- Routers: Wired/Wireless

- Switches: Managed/Unmanaged

- Firewalls: Hardware/Software

- Connectivity: Ethernet, Wi-Fi

Risks:

- Data breaches

- Network downtime

- Configuration errors

- Device tampering

- Power outages

Mitigation:

- Secure network configuration

- Regular firmware updates

- Password protection

- Network monitoring

- Redundant power sources

Common Risks and Mitigations:

- Data breaches: Secure network configuration, encryption, regular software updates

- Device tampering: Tamper-proof housing, secure connections

- Power outages: Redundant power sources, UPS

- Maintenance costs: Regular maintenance, replacement schedules

- User errors: Training, documentation