

INFORMATION SECURITY MANAGEMENT

ASSIGNMENT



**NAME : S.PAVITHRA**

**REGISTER NUMBER : 23370043**

**COURSE CODE : CSEL 446**

**DEPARTMENT : M.SC CS(2nd Year)**

**SEMESTER : THIRD SEMESTER**

ASSET MANAGEMENT

What Is an Asset?

An asset is a resource with [economic value](https://www.investopedia.com/terms/e/economic-value.asp) that an individual, a company, or a country owns or controls with the expectation that it will provide a future benefit.

**Key Takeaways**

* An asset is a resource that is expected to provide a future benefit to its owner.
* In the case of businesses, assets are reported on the company's balance sheet.
* An asset may generate cash flow, reduce expenses, or improve sales, and it may be either tangible (like a piece of machinery) or intangible (like a copyright).
* For accounting purposes, assets are commonly classified as current, fixed, financial, or intangible.

**1. Purpose**

To ensure efficient, effective, and responsible management of university-owned IT assets.

To maintain accountability and transparency in managing IT resources.

To support sustainable practices and ensure compliance with legal, regulatory, and university standards.

**2. Scope**

This policy applies to all IT assets, including hardware, software, and digital resources owned or managed by the university.

It covers all university departments, faculty, staff, and students who access or use university IT assets

**3. Asset Types**

* Computers
* Server Switch
* CCTV Cameras
* Routers
* Network switch
* Operating Systems
* Ethernet
* Uninterruptible Power Supplies (UPS)
* Printers
* Projectors and Display Screens

**1)ASSET NAME :** Computers

**OWNER :** Head of the Department

**ROLE :**  Educational Resource Access

**RISK :**  Unauthorized access to sensitive data by employees or external agents can lead to data leaks or misuse of asset information**.** Non-compliance with regulations like GDPR or financial reporting standards can lead to penalties, legal issues, and reputational damage.

**MITIGATION :** Limit access based on job roles and monitor user activity. Implement identity verification measures like biometric authentication and routinely update access controls as roles change. Stay informed about relevant regulations and use compliance management tools to monitor adherence. Regularly review policies and procedures and conduct internal compliance audits.

**2)ASSET NAME :** Server Switch

**OWNER :** Head of the Department

**ROLE :** Network Traffic Management

**RISK** : Loss of power to server switches can bring the entire network down, interrupting operations and potentially causing data loss. High temperatures can cause switch hardware to fail or perform poorly, especially in densely packed server environments.

**MITIGATION** : Use Uninterruptible Power Supplies (UPS) to provide backup power, and consider redundant power sources or generators for critical switches. Maintain proper ventilation and cooling in server rooms, monitor temperatures, and set up automated alerts for environmental conditions.

**3)ASSET NAME :** CCTV Cameras

**OWNER** : Head of the Department

**ROLE :** Surveillance and Monitoring

**RISK :** Maintaining and upgrading CCTV systems can be costly, including hardware, software, and storage costs, especially if a large area needs coverage. Technical failures, power issues, or poor maintenance can cause outages, reducing the system’s effectiveness.

**MITIGATION :** Conduct regular checks and maintenance of CCTV equipment to ensure optimal functioning. Implement monitoring systems to detect any system downtime immediately. Use encrypted storage solutions and implement access controls to protect sensitive footage. Regularly back up footage and ensure it is securely archived.

**4) ASSET NAME :**  Routers

**OWNER :** Head of the Department

**ROLE :** Network Connectivity

**RISK** : Improperly configured routers may expose sensitive data to external threats, increasing the risk of data breaches. Routers can be targets for cyber-attacks like DDoS attacks, unauthorized access, and malware, potentially compromising connected assets.

**MITIGATION :** Use strong passwords, two-factor authentication (2FA), and network segmentation to restrict access to routers and sensitive data. Encrypt data transmitted through routers to ensure secure communications, reducing the risk of interception.

**5) ASSET NAME :** Operating Systems

**OWNER :** Faculty Department

**ROLE :** An operating system (OS) manages computer hardware and software resources, enabling efficient operation and user interaction.

**RISK :** Data can be lost due to system crashes, accidental deletion, or hardware failure. OS vulnerabilities can be exploited by attackers to gain unauthorized access, steal data, or install malware.

**MITIGATION :** Implement automatic and frequent backups to protect important data. Keep the OS and software up-to-date with the latest security patches. Enable firewalls and use reliable antivirus software to detect and block threats.

**6) ASSET NAME :** Network Switch

**OWNER :** Head of the Department

**ROLE :** Switches enable communication between devices by directing data packets to the correct device on the network.

**RISK :** Switches, if improperly secured, can be entry points for attackers to intercept or reroute network traffic. Loss of power to server switches can bring the entire network down, interrupting operations and potentially causing data loss.

**MITIGATION :** Use network monitoring tools to detect unusual traffic patterns or issues early on, and regularly audit configurations to maintain optimal performance**.** Use Uninterruptible Power Supplies (UPS) to provide backup power, and consider redundant power sources or generators for critical switches.

**7) ASSET NAME :** ETHERNET

**OWNER :**  Lab Administrator

**ROLE :** Provides reliable and fast data transfer between computers, servers, and network devices. Ethernet enables direct physical connections, reducing the risk of interference and unauthorized access compared to wireless networks.

**RISK :** Unsecured Ethernet ports can be an entry point for unauthorized users, leading to data breaches or compromised network security. High usage, especially in a shared lab environment, can lead to bandwidth congestion, affecting network performance.

**MITIGATION :** Limit access to Ethernet-connected devices and areas with sensitive data to authorized personnel only. Disable unused ports and use MAC address filtering to limit access to trusted devices.

**8) ASSET NAME** : Uninterruptible Power Supplies (UPS)

**OWNER** : Head of the Department

**ROLE :** Provides temporary power during outages, ensuring continuous operation of lab computers, servers, and networking equipment. Allows users time to save work and safely shut down equipment during power interruptions, preventing data loss and potential file corruption.

**RISK**  : If too many devices are connected or the UPS capacity is insufficient, it may fail to support all devices during a power interruption. UPS units can be affected by temperature, humidity, and dust, leading to reduced efficiency or premature failure.

**MITIGATION**  : Ensure the UPS capacity matches the power needs of connected equipment, and avoid overloading. Implement a maintenance schedule for testing, cleaning, and inspecting UPS units. Install UPS units in a well-ventilated, temperature-controlled area.

**9) ASSET NAME :** Printers

**OWNER :** Head Of The Department

**ROLE** : Provides essential printing services for students, faculty, and staff for assignments, reports, and research documents. Supports academic tasks by converting digital files to hardcopies for presentation, review, or offline study.

**RISK :** Printers can be accessed by unauthorized users, leading to data theft or misuse, particularly if sensitive documents are printed. Frequent use can lead to high maintenance costs and rapid depletion of consumables like ink, toner, and paper. Printers generate waste from ink/toner cartridges, paper, and energy consumption

**MITIGATION** : Implement PIN codes or access card authentication for users. Invest in energy-efficient printers that reduce costs and environmental impact. Use recycling programs for cartridges and encourage double-sided printing to reduce paper waste.

**10) ASSET NAME :** Projectors and Display Screen

**OWNER :** Head Of the Department

**ROLE :** Projectors and screens are used to display instructional material, presentations, and media, enhancing learning and collaboration. They provide visual support for lectures, training, and demonstrations, making complex concepts easier to understand.

**RISK :** Projectors and screens are susceptible to accidental damage from drops, bumps, or mishandling, as well as from environmental factors like dust or heat. Projectors and screens can experience degraded image quality due to dust buildup, lens scratches, or outdated technology, affecting the user experience. Projectors, especially high-quality models, can be expensive to replace and maintain, adding to operational costs.

**MITIGATION :** Keep projectors and screens in dust-free, well-ventilated areas to prevent overheating and dust accumulation. Clean lenses and screens routinely to maintain image clarity. Upgrade equipment according to technology standards to maintain high-quality displays. Track projector usage to anticipate bulb replacement schedules