INFORMATION SECURITY MANAGEMENT

ASSIGNMENT

NAME : K.SHREE VARSHNIE

DEPARTMENT : MSC COMPUTER SCIENCE

REG NO : 23370057

DATE : 28/10/2024

ASSET MANAGEMENT

ASSET NAME : SERVER SWITCH

OWNER : Head of Department

ROLE : The server switch role is to facilitate high-speed data communication between servers and devices in a network, ensuring efficient data routing and minimizing latency.

USES : Server switches are used to connect and manage data traffic between multiple servers within a network, optimizing communication and resource allocation for efficient data transfer.

RISK : Server switches are at risk of network failures, unauthorized access, and misconfigurations, which can disrupt data communication and compromise security.

MITIGATION : The server switch role is to facilitate high-speed data communication between servers and devices in a network, ensuring efficient data routing and minimizing latency.

ASSET NAME : ROUTERS

OWNER : Head of Department

ROLE : Routers connect and direct data traffic between different networks, enabling devices to communicate efficiently and securely.

USES : Routers are used to connect different networks, directing data packets between them to facilitate communication and internet access for connected devices.

RISK : Routers are at risk of cyberattacks, such as unauthorized access and DDoS attacks, which can disrupt network connectivity and compromise sensitive data.

MITIGATION : Router mitigation involves employing security measures such as firewalls, regular firmware updates, and network segmentation to protect against unauthorized access and cyber threats.

ASSET NAME : PORTS

OWNER : Head of Department

ROLE : Ports facilitate communication between networked devices by serving as specific endpoints for different types of data traffic and services.

USES : Ports are used to identify specific communication endpoints on devices, enabling different types of data traffic to flow to and from applications and services over a network.

RISK : Ports are at risk of exploitation through unauthorized access and attacks, such as port scanning and DDoS attacks, which can compromise network security and disrupt services.

MITIGATION : Port mitigation involves closing unused ports, employing firewalls, and implementing access controls to reduce vulnerabilities and prevent unauthorized access to network services.

ASSET NAME : COMPUTERS

OWNER : Head of Department

ROLE : Computers process, store, and manage data, enabling users to perform a wide range of tasks and facilitating communication, productivity, and innovation across various fields.

USES : Computers are used for processing data, running applications, and facilitating communication across various fields, enhancing productivity and driving innovation.

RISK : Computers are at risk of malware infections, cyberattacks, and hardware failures, which can lead to data loss, security breaches, and disrupted operations.

MITIGATION : Computer mitigation involves implementing robust security measures, regular software updates, and data backup solutions to protect against malware, data breaches, and system failures.

ASSET NAME : AUTHENTICATION

OWNER : Head of Department

ROLE : Authentication verifies the identity of users or systems to ensure that only authorized individuals can access sensitive resources and information.

USES : Authentication is used to verify the identity of users or systems, ensuring that only authorized individuals can access sensitive resources and data.

RISK : Authentication is at risk from phishing attacks and weak password practices, which can lead to unauthorized access and data breaches.

MITIGATION : Authentication mitigation involves implementing multi-factor authentication and strong password policies to enhance security and reduce the risk of unauthorized access.

ASSET NAME : SERVERS

OWNER : Head of Department

ROLE : Servers provide centralized resources and services, managing data storage, processing, and communication for multiple clients or devices within a network.

USES : Servers are used to host applications, manage databases, and provide resources and services, enabling users and devices to access data over a network.

RISK : Servers are at risk of cyberattacks, data breaches, and hardware failures, which can compromise sensitive information and disrupt critical services.

MITIGATION : Server mitigation involves using redundancy, regular updates, and robust security measures to protect against failures and unauthorized access while ensuring data availability.

ASSET NAME : OPERATING SYSTEM

OWNER : Head of Department

ROLE : The operating system acts as an intermediary between hardware and user applications, managing resources and providing a user interface for seamless interaction with the computer.

USES : Operating systems are used to manage computer hardware and software resources, providing a user interface and enabling applications to run efficiently.

RISK : Operating systems are at risk of malware attacks, vulnerabilities from outdated software, and misconfigurations that can lead to unauthorized access and data breaches.

MITIGATION : Operating systems mitigation involves regularly updating software, implementing strong security configurations, and using antivirus tools to protect against vulnerabilities and cyber threats.

ASSET NAME : ETHERNET

OWNER : Head of Department

ROLE : Ethernet serves as a fundamental networking technology that facilitates wired communication between devices in a local area network (LAN) by transmitting data packets over physical cables.

USES : Ethernet is used to connect devices within local area networks (LANs), enabling high-speed data transfer for applications like internet access, file sharing, and networked printing.

RISK : Network switches are at risk of security vulnerabilities, unauthorized access, and misconfigurations that can disrupt network performance and compromise data integrity.

MITIGATION : Ethernet mitigation involves implementing network segmentation, using VLANs, and employing security measures such as firewalls and intrusion detection systems to protect against unauthorized access and data breaches.

ASSET NAME : NETWORK SWITCH

OWNER : Head of Department

ROLE : The network switch role is to connect devices within a local area network (LAN) and direct data packets between them to optimize communication and resource sharing.

USES : Network switches are used to connect multiple devices in a local area network (LAN), facilitating efficient data transfer and communication between them.

RISK : Network switches are at risk of security vulnerabilities, unauthorized access, and misconfigurations that can disrupt network performance and compromise data integrity.

MITIGATION : Network switch mitigation involves implementing security measures like VLAN segmentation, access controls, and regular monitoring to protect against unauthorized access and network congestion.

ASSET NAME : DATABASE

OWNER : Head of Department

ROLE : The role of a database is to store, organize, and manage data efficiently, allowing users and applications to retrieve and manipulate information as needed.

USES : Databases are used to store and manage structured data, enabling quick retrieval, updates, and analysis for applications in various fields like business, healthcare, and finance.

RISK : Databases are at risk of unauthorized access, data breaches, and corruption, which can lead to loss of sensitive information and operational disruptions.

MITIGATION : Database mitigation involves using encryption, access controls, and regular backups to protect data integrity, prevent unauthorized access, and ensure data availability.