AAQ IT Unit 2: Cyber Security and Incident Management

A4: Hardware and Software Security Measures

Rons Tech Hub

Software and Hardware Security Measures

Rons Tech Hub

Organisations use security measures to protect systems, devices, and data.

Security measures can be physical, software-based, or network-based.

Good security reduces the risk of attacks and data loss.

Multiple layers of security provide the best protection.

Physical Security Measures

- Physical security protects buildings, equipment, and people.
- Site security can include locks, alarms, CCTV, and security staff.
- These measures help prevent unauthorised access.
- Physical security is often the first line of defence.

Access Control Systems

- Buildings may use card entry systems to control access.
- Technologies include NFC, RFID, magnetic stripe cards, and QR codes.
- Embedded chips can store security information securely.
- Only authorised users should be able to enter restricted areas.

Rons Tech Hub

Biometric Security

- Biometrics use physical characteristics to identify users.
- Examples include fingerprints, facial recognition, and iris scans.
- Voice recognition and signature recognition can also be used.
- Biometric systems are difficult to copy or share.

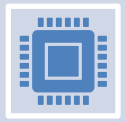
Protecting Equipment

- Equipment should be protected using secure cabinets and protected cabling.
- Devices may also have alarms to detect theft or tampering.
- CCTV can help monitor sensitive areas.
- Staff training helps reduce human security mistakes.

Rons Tech Hub

Backups and Recovery

Backups create copies of important data.



They help organisations recover after data loss or cyber attacks.

Recovery procedures restore systems and information.

Regular backups are an important security measure.

Types of Backup

Rons Tech Hub

A full backup copies all selected data.

A differential backup copies changes since the last full backup.

An incremental backup copies changes since the last backup.

Incremental backups are usually the fastest to perform.

Backup Strategies

Rons Tech Hub

Backups can be stored onsite, offsite, or in the cloud.

Some backups run automatically while others are manual.

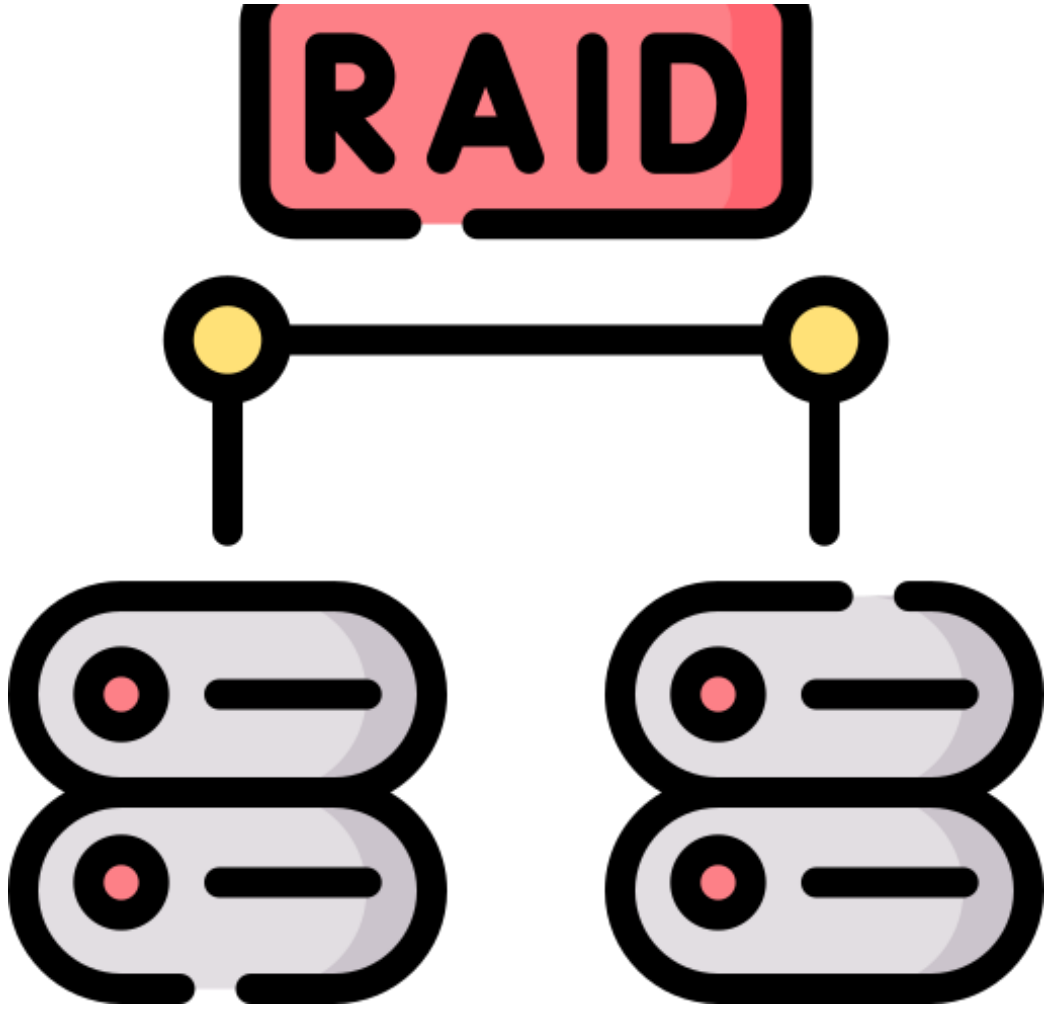
Hot sites can be used immediately after a disaster.

Warm sites need some setup before becoming operational.

Rons Tech Hub

Backup, Archiving and RAID

- Backups are used to recover lost data.
- Archives store old data that may be needed later.
- RAID improves data availability using multiple drives.
- RAID is not a replacement for a backup.



Recovery Methods

Rons Tech Hub

- Individual files can be restored when needed.
- Entire devices can be restored from system images.
- Bare-metal recovery restores a complete system from scratch.
- Recovery plans reduce downtime after incidents.

Rons Tech Hub

Antivirus Software

- Antivirus software detects and removes malicious software.
- It scans files and monitors system activity.
- Regular updates improve protection against new threats.
- Antivirus software is an important security tool.

Antivirus Detection Methods

Rons Tech Hub

- Signature-based detection compares files against known malware patterns.
- Heuristic analysis looks for suspicious behaviour.
- File integrity checks detect unexpected file changes.
- Checksums help identify whether files have been altered.

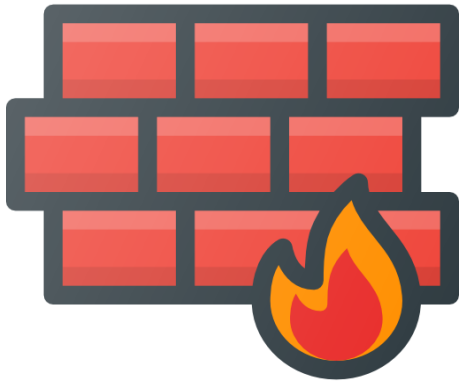
Responding to Threats

- Security software may warn users about threats.
- Threats can be logged for investigation.
- Malicious files may be blocked from running.
- Dangerous files can be quarantined or deleted.

Rons Tech Hub

Rons Tech Hub

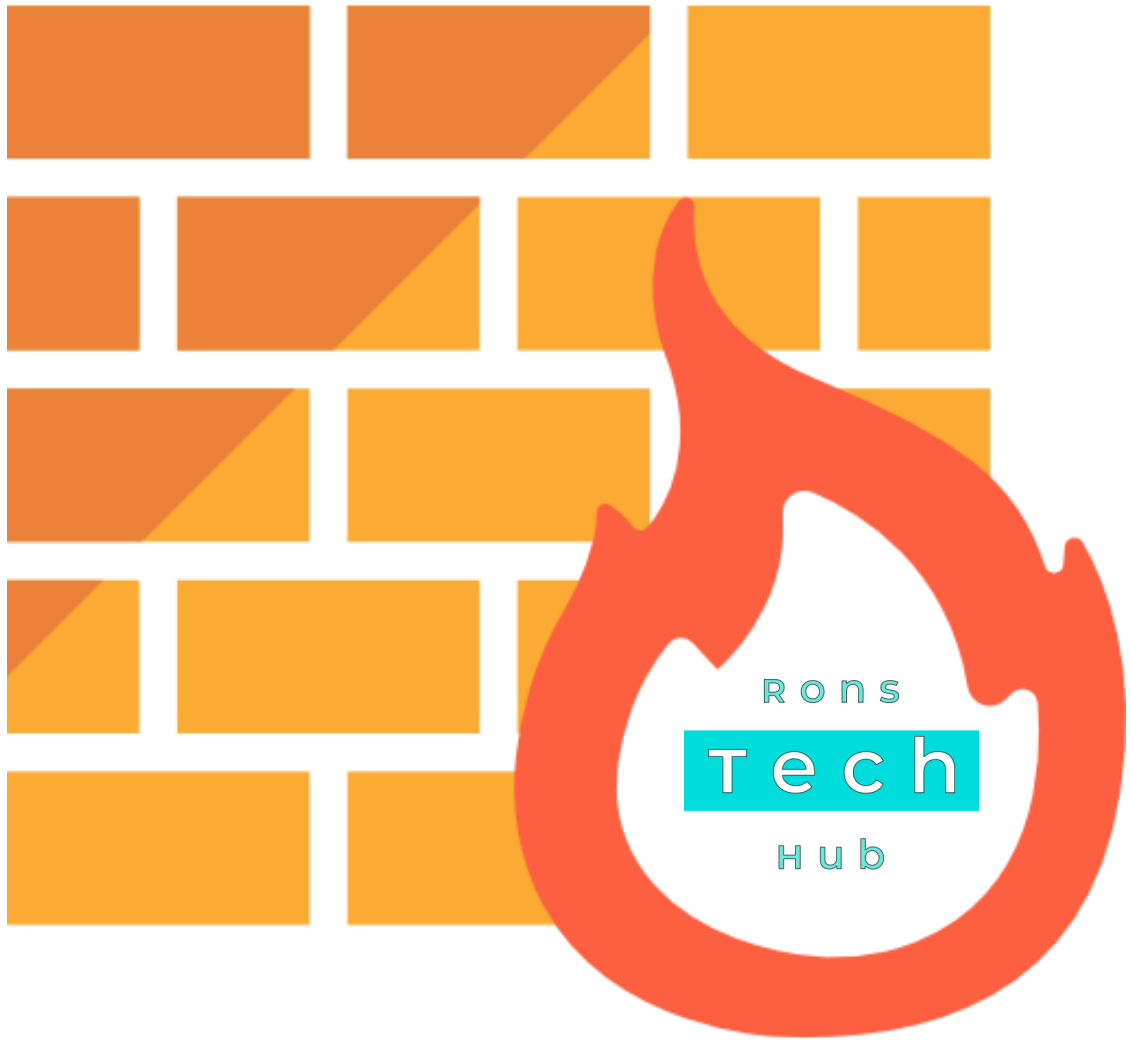
Firewalls



- Firewalls monitor and control network traffic.
- They help prevent unauthorised access to systems.
- Firewalls can be hardware devices or software applications.
- Most organisations use both types together.

Firewall Filtering Techniques

- Packet filtering checks information in network packets.
- Inspection techniques examine traffic more closely.
- Application-aware firewalls understand specific applications.
- Rules control both incoming and outgoing traffic.

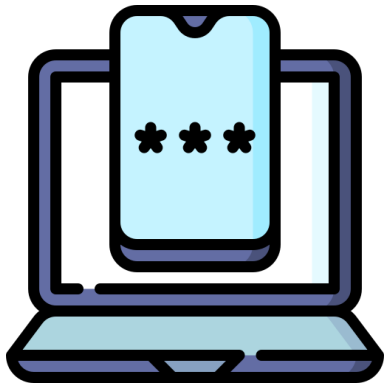


Rons Tech Hub

User Authentication

- Authentication confirms that a user is who they claim to be.
- Most systems require a username and password.
- Strong passwords help prevent unauthorised access.
- Password policies improve account security.

Multi-Factor Authentication (MFA)



MFA uses two or more methods to verify identity.

Knowledge factors are things you know, such as passwords.

Possession factors are things you have, such as a phone.

Inherence factors are things you are, such as fingerprints.

Rons Tech Hub

Security Tokens

- Security tokens provide an extra layer of authentication.
- Some tokens are USB devices or smart cards.
- Others generate codes using an app or dedicated device.
- Banks commonly use token-based authentication.

Kerberos Authentication

Rons Tech Hub

Kerberos is a network authentication system.

A client requests access from a server.

The server verifies the user's identity and exchanges keys securely.

Kerberos is commonly used in Windows and Linux networks.

Digital Certificates

Rons Tech Hub

Digital certificates help prove the identity of websites and systems.

Certificates are issued by trusted Certificate Authorities (CAs).

TLS encrypts data travelling across networks.

HTTPS uses certificates to secure websites.

Access Controls

- Access controls restrict what users can see and do.
- Permissions can apply to files, folders, applications, and devices.
- Access should be based on job requirements.
- Limiting access reduces security risks.

Rons Tech Hub

DAC, Role-Based and Rule-Based Access Control

- DAC allows users to control access to their own resources.
- Role-Based Access Control assigns permissions based on job roles.
- Rule-Based Access Control uses rules set by administrators.
- These methods help manage permissions efficiently.

Trusted Computing and Device Security

- Trusted computing can improve system security and reliability.
- A disadvantage is reduced user control and privacy.
- Devices can automatically lock after inactivity.
- Failed login attempts may trigger lockouts or data wipes.

Rons Tech Hub

Finding Lost or Stolen Devices

GPS can help locate missing devices.

Some devices report their location when connected to the internet.

Tracking software can monitor device movements.

Remote tools can lock or wipe stolen devices.

Rons Tech Hub

Rons Tech Hub

Encryption

- Encryption converts readable data into unreadable data.
- Only authorised users can decrypt the information.
- Encryption protects data stored on devices.
- It also protects data sent across networks.

Rons Tech Hub

Storage and Communication Encryption

- Storage encryption can protect files, folders, discs, and devices.
- AES is a common symmetric encryption standard.
- RSA uses public and private keys for asymmetric encryption.
- Diffie-Hellman helps devices exchange encryption keys securely.

Secure Communication Technologies

Rons Tech Hub

- VPNs create secure connections across public networks.
- HTTPS protects communication between browsers and websites.
- End-to-End Encryption protects messages from interception.
- TOR helps increase privacy when browsing online.

Protecting Wireless Networks

- WLANs can be protected using WPA2 or WPA3 encryption.
- MAC address filtering restricts which devices can connect.
- Administrators should change default passwords and settings.
- Firewalls and VPNs provide additional protection.

Rons Tech Hub

Wireless Threats

- Unsecured access points can allow unauthorised access.
- Piggybacking occurs when someone uses a network without permission.
- Evil Twin attacks use fake wireless access points.
- Wireless sniffing can capture network traffic.

RONS TECH HUB

Secure Network and System Design

Security should be considered from the start of system design.

Organisations should assume attacks will happen and plan accordingly.

Systems should follow the principle of least privilege.

Security standards such as ISO 27000 help organisations manage risks.

Rons Tech Hub