Level 1/2 Vocational

ICT

1.3.3 Methods used to protect information

Logical protection

Logical protection uses computer-based methods to secure systems and information, preventing unauthorised access or limiting authorised user access.

- **Access levels:** Different users are given varying permissions. This ensures employees only see information relevant to their role (for example finance staff see salaries while others do not). Access can be set to 'read only' or 'edit'.
- **Authentication:** The process of proving your identity to a system.
  - **Two-factor authentication:** After entering a username and password, a code is sent (for example to email) which must be entered to confirm identity.
  - **Other methods:** PINs, secret questions and biometrics (for example fingerprints or facial recognition).
- **Firewalls:** Monitor all incoming and outgoing network traffic. They compare this data against set rules to block unauthorised access and prevent malicious traffic from entering or leaving a system. Firewalls can be software, hardware or built into an operating system.
- **Anti-malware applications:** Programs designed to identify and deal with malware (for example viruses or spyware).
  - They compare data against a database of known malware.
  - They must be updated regularly due to new threats.
  - They can prevent malware downloads or notify users to quarantine or remove existing malware.
  - Heuristic analysis: Detects unknown viruses by examining code for suspicious properties or behaviour.
- **Password protection:** Passwords allow access only to authorised users. A password entered is compared to one stored in a database. If incorrect, access is denied. Systems may lock after multiple failed attempts.

Strong passwords are crucial:

- Unique for different applications.
- Complex: mix of letters (upper/lower), numbers, symbols.
- Long (usually at least eight characters).
- Not easily guessed (e.g., pet's name).

Password managers can create and store complex passwords securely.
Users may be notified if their passwords are compromised in data breaches.

- **Encryption:** Encryption scrambles data (plain text) into an unreadable format (cyphertext) using an algorithm. This prevents unauthorised users from understanding it if intercepted. A special key is needed to decrypt the cyphertext back to plain text.
  - Symmetric encryption: Uses a single key for both scrambling and unscrambling. Faster but less secure.
  - Asymmetric encryption: Uses two different keys. Slower but more secure.

Physical protection

Physical protection uses tangible methods to keep your data safe rather than digital methods.

- **Locks**: Secure rooms where hardware or backups are kept (for example server rooms or computer rooms). These can use traditional keys, codes, key cards or biometrics.
- **Biometrics:** Use unique human characteristics (for example fingerprints, iris scans or facial recognition) for access control. Convenient as no keys or cards are needed, and identification cannot be shared.
- **Location of hardware:** Store computers in a safe place, protected from fire, flooding and large windows. Rooms should be cool and well ventilated to prevent overheating.
- **Security staff:** Employed in large organisations to patrol and monitor computer systems, especially where sensitive information is stored, for example government departments.
- **Backup systems:** Data should be backed up regularly and stored securely, away from the main computer system, to ensure data recovery if primary systems are damaged.

Security policies

Written documents outlining how an organisation protects itself against security threats.

- **Disaster recovery plan:** A formal policy detailing how an organisation will respond to catastrophic events (for example cyberattacks, natural disasters or power cuts). Aims to minimise damage and quickly restore operations. Disaster recovery plans include preventative ('before') and response ('during') phases.
- **Staff responsibilities:** Employees must understand and follow security policies.
- **Acceptable Use Policy (AUP):** Defines what users can and cannot do on the organisation's computer system (e.g. use of removable drives or social media access). Employees usually agree to the AUP before gaining system access.
- **Staff training:** Crucial for employees to keep up with evolving IT systems, software and procedures. Ensures consistent work practices across the organisation. Training can include courses, conferences, seminars or work shadowing.

Emerging technologies

New technologies are constantly developing to combat cybercrime and ensure secure operations, especially with the rise of remote working.

One emerging technology is confidential computing. This technology uses a hardware-based environment to isolate and protect data even while it is being processed (after decryption). It provides end-to-end data protection across the at rest, in transit and in use phases.