1. Data Security

6	Security, privacy and data integrity	
6.1	**Data Security**	
Candidates should be able to:		Notes and guidance
Explain the difference between the terms security, privacy and integrity of data		
Show appreciation of the need for both the security of data and the security of the computer system		
Describe security measures designed to protect computer systems, ranging from the stand-alone PC to a network of computers		Including user accounts, passwords, authentication techniques such as digital signatures, firewall, anti-virus software, anti-spyware, encryption
Show understanding of the threats to computer and data security posed by networks and the internet		Including malware (virus, spyware), hackers, phishing, pharming
Describe methods that can be used to restrict the risks posed by threats		
Describe security methods designed to protect the security of data		Including encryption, access rights

---

- Security vs privacy vs integrity
  - Security
    - Security is keeping data safe from accidental damage
    - Security is the prevention of data loss
  - Privacy
    - Privacy is the need to restrict access to personal data/keep data confidential
    - To avoid being seen by unauthorized people
  - Integrity
    - Integrity is making sure the data is correct / valid / accurate / consistent / up-to-date
    - Integrity ensures that the data received is the same as the data sent
- Security measure
  - User accounts and password
  - Digital signatures
  - Firewall
    - Examine the traffic between the computer and the internet

        - Check whether incoming or outgoing data meets a given set of criteria
        - Block the traffic if the data fails to meet the criteria, and giving the user a warning
        - Log all incoming and outgoing traffic to allow later interrogation
        - Prevent access to certain undesirable sites
        - Helps to prevent viruses or hackers
        - Sent warning if some software is trying to access an external data source
    - Anti-virus software
        - Check software before they run on a computer
        - Compare possible virus against a database of known viruses
        - Carry out heuristic checking
        - Quarantine files which are possibly infected
    - Anti-spyware
    - Encryption
        - Data are scrambled so they cannot be understand unless a decryption key is given
- Security threats
    - Malware (virus, spyware)
        - Virus
            - Malicious program
            - Replicates itself
            - Can cause loss of data
            - Can cause computer to crash
            - Can fill up hard disk with data
        - Spyware
            - Gathers information by monitoring key presses on user's keyboard
    - Hacker
        - Illegal access to a computer system without the user's permission. Intentional delete, alter or corrupt user's files, or to gain personal information
    - Phishing
        - Legitimate-looking emails containing links or attachments which, when clicked, take the user to fake website, or they may trick the

user into responding with personal data
    - Pharming
        - Malicious code installed on a user’s computer or web server, redirects to a fake website without their knowledge and gain personal information
- Security methods
    - Encryption
    - Access rights
