1. A backup of a server is made each night. Only the files changed that day are backed up.

Identify the name of this type of backup.

(1)

A Fragmented **B** Full **C** Incremental **D** Lossy

2. Explain **one** reason why files should be backed up regularly. **(2)**

3. Students are asked to sign an acceptable use policy.

Explain **one** way that an acceptable use policy helps to protect student data.

(2)

4. Describe an acceptable use policy (AUP).
(1)

5. Give 3 ways that an organisation can protect data. **(3)**

6. Explain how encryption can be used to protect data. **(2)**

7. Give 2 physical methods that an organisation can use to protect data. **(2)**

8. Which of the following is an effective way for an organization to protect its data? **(1)**

A Storing all data on a single device
B Using strong passwords and multi-factor authentication
C Allowing employees to share login details
D Providing unlimited access to all employees

9. What is the purpose of data encryption in an organization's data protection strategy? **(1)**

A To prevent all data access by employees
B To ensure data is never lost or deleted
C To secure data from unauthorized access and hacking
D To share data with external parties more easily

10. Describe the purpose of RAID in managing data.

ANSWERS

A backup creates a copy of data/files that is kept in A DIFFERENT LOCATION to the original files. Backups allow data to be restored if the original data is compromised in some way (cyber attack or physical destruction)

1. C Incremental backup backs up all files that have been created or edited since the last backup. A full backup backs up everything. Incremental backups are faster.

2. Files should be backed up regularly to ensure that data can be restored in case of data loss. Backups also protect against ransomware because a company doesn't have to pay for data to be decrypted if they have their own backup. Loss of data with no backup could be the end of a company.

3. An Acceptable Use Policy sets out the rules of using a network. It covers issues including security of a network and protection of data. By students signing an AUP they are educated about responsible network use and reminded that they are accountable for their actions on the network.

4. An Acceptable Use Policy is a set of rules for using technology. It tells people what they can and cannot do with computers, networks, and the internet. Think of it as a guidebook that helps everyone use these tools responsibly and safely.

5. Restrict access to data – user access rights, strong passwords, locked server rooms (biometrics, keypads), CCTV, fences, security guards, firewall
   Encryption so that if data falls into the wrong hands it cannot be read.
   Backup – so that if data is lost, it can quickly be restored.

6. Encryption is the scrambling of data using a key. The data can only be decrypted by a person or organisation that has the same key. Encryption protects data because it stops it being read by unauthorised people even if it is accessed. An example of encryption protecting data is when the HTTPS protocol is used to send data over the internet.

7. Physical methods to protect data include locked offices using biometric entry, CCTV, a physical hardware-based firewall.

8. B

9. C

10. **RAID** stands for Redundant Array of Independent Disks**.** What it means is storing data on multiple hard drives rather than all on one. This allows data to be protected in case of a hard drive failure. RAID is different to back up because it doesn't allow data to be restored in case of situations like ransomware. It is only there in case of disc failure.