

Name _____

Exploring the Security of Cloud Computing

Short Answer Key

1. Data encryption in cloud computing involves converting data into a coded format to protect it from unauthorized access. It is important for security because it ensures the confidentiality of sensitive information by making it unreadable without the proper decryption key.
2. The shared responsibility model in cloud security means that security responsibilities are divided between the cloud provider and the customer. While the provider secures the underlying infrastructure, customers are responsible for securing their data and configuring access controls properly.
3. One physical security measure that cloud data centers employ is biometric access controls. These controls require authorized individuals to use their unique biometric characteristics, such as fingerprints or retina scans, to gain access to the data center.
4. Redundancy and disaster recovery ensure data security and availability in the cloud by maintaining multiple copies of data in different locations. In the event of hardware failures or disasters, data can be quickly restored from backups, minimizing downtime.
5. Organizations can enhance cloud computing security by implementing strong passwords, educating employees on security practices, regularly monitoring and auditing their cloud environments, and adhering to compliance standards.

