

To ensure the network and connected systems are available 24/7, reliable, and can recover quickly in case of interruptions, the network security administrator should implement the following strategies: 1. By implementing these strategies, the network security administrator can effectively protect the company's data, systems, and operations, ensuring availability, reliability, and quick recovery in the face of potential threats or interruptions.

- Physical Security**: – Secure physical access to network components such as servers, routers, and switches by implementing measures like biometric authentication, access control systems, and surveillance cameras.
- Password Management**: – Enforce strong password policies requiring complex passwords that are regularly updated.– Utilize digital signatures and certificates to authenticate users and devices.
- Antiviruses**: – Install and regularly update antivirus software on all network-connected devices.– Implement environmental controls to safeguard networking equipment from physical threats like fire, water damage, and power surges.
- Cryptography (Encryption and Decryption)**: – Encrypt sensitive data both in transit and at rest using secure encryption algorithms.– Implement email filtering to prevent phishing attacks and malware distribution.– Implement automated backup solutions to avoid human errors and ensure consistency.– Implement multi-factor authentication .to add an extra layer of security.2.3.4.5.6.7