Core Security Principles

Confidentiality: Ensure only AUTHORIZED USERS CAN ACCESS RESOURCES.

Integrity: Ensures DATA IS ACCURATE AND UNMODIFIED.

Availability: Ensures resources are AVAILABLE FOR AUTHORIZED USERS.

Non-Repudiation: Users CANNOT deny that they something when there's proof they did. (e.g., logs)

Defense in Depth

Implementing multiple layers of security controls to protect assets. If one control fails, others are in place to prevent breaches.

Least Privilege

Granting users only the minimum level of access required to perform their job duties.

Zero Trust

"Never Trust, Always Verify". Treat every connection attempt as a potential threat

Core Security Principles

Authentication, Authorization and Accountability

Authentication: Validate the identity of the user.

Types of Authentication

Single factor authentication	One method of authentication. (Username + Password)
Multi Factor Authentication	Requiring two or more verification factors (something you know, something you have, something you are) to access resources.

Authentication Techniques

Type 1: Something you know	PIN or Passwords

Core Security Principles (cont)

Type 2: Something you have	Tokens, Smart Cards
Type 3: Something you are	Biometrics

Authorization: Grants the user rights based on their role

Accounting: Audits log access