CIA Triad (Confidentiality, Integrity, Availability)

The **CIA Triad** represents the three **core principles of information security** that guide the design and evaluation of security policies, systems, and practices.

CIA Triad Principles

Confidentiality

Ensuring that **information is accessible only to authorized individuals** and protected from unauthorized access or disclosure.

Ex: Encryption of sensitive data.

Integrity

Ensuring the **accuracy, consistency, and trustworthiness of data** across its lifecycle. Data must not be improperly modified or destroyed.

Ex: Checksum, digital signatures.

Availability

Ensuring that **authorized users have reliable and timely access to resources** when required. The system must remain operational and functional.

Ex: Redundant servers, DDoS protection.

IAAAA (Identification, Authentication, Authorization, Accountability, Auditing)

Identification

The process where a user claims an identity

Ex: Entering a username or ID during login.

Authentication

Verifying the user's claimed identity using credentials. Ex: Entering password, OTP, biometric

Authorization

Determining what actions or resources the authenticated user is allowed to access. Ex: Access control lists (ACL), role-based access control (RBAC).

Accountability

Holding users responsible for their actions within a system; users must be uniquely identified and tracked.

Ex: User-specific logs, session IDs.

Auditing

Logging and reviewing activities to detect abnormal or malicious behavior and ensure compliance.

Ex: Log reviews, security audits.