The CIA Triad – Core Principles of Cybersecurity

The CIA Triad represents three main goals of cybersecurity: **Confidentiality, Integrity, and Availability.** These principles ensure data and systems remain secure, accurate, and accessible.

■ Confidentiality

Confidentiality means keeping information private and safe from unauthorized access.

Example: Using passwords, encryption, and access control. Hiding customer data from public access.

Purpose: To prevent sensitive information from being viewed by the wrong people.

■■ Integrity

Integrity ensures data is accurate, complete, and unchanged from its original form.

Example: Using hashing or digital signatures. Checking data consistency during transfer.

Purpose: To protect information from being altered or corrupted by unauthorized users.

■ Availability

Availability ensures that data and systems are accessible to authorized users when needed.

Example: Using backups, redundant systems, and disaster recovery plans. Maintaining servers and networks.

Purpose: To make sure information and services are always available for use.

■ Summary

Principle	Focus	Example Tools/Methods
Confidentiality	Keep it secret	Passwords, Encryption
Integrity	Keep it correct	Hashing, Digital Signatures
Availability	Keep it usable	Backups, Redundant Systems

■ Why the CIA Triad Matters

The CIA Triad helps organizations maintain **trust**, **reliability**, and **resilience** in their systems. Strong cybersecurity depends on balancing all three principles effectively.