

## **Confidentiality, Integrity, and Availability (CIA) Triad**

**Some common methods used to ensure Confidentiality, Integrity, and Availability properties for information security and secure software systems:**

<b>Confidentiality</b>	<b>Integrity</b>	<b>Availability</b>
Encryption	File permissions	Maintaining and upgrading both hardware and system software
User ID and Password	User access controls	Adequate communication bandwidth to prevent bottlenecks
Two-factor authentication	Version control	Redundancy, failover, RAID (redundant array of independent disks), high availability (HA) clusters
Biometric verification	Checksums	Backups stored in a geographically-isolated location
Security tokens	Cryptographic checksums (also known as message authentication codes)	Firewalls, proxy servers, IP filtering to defend against DoS attacks and network intrusions.
Key fobs	Backups (to restore affected data)	Disaster recovery plans
Soft tokens	Hash functions	
Using air gapped computers and disconnected storage devices		
Limiting the number of times data is shown and/or transmitted		

Sources:

- <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>