CIA (Confidentiality, Integrity, Availability)

Confidentiality -> ensure that sensitive information is not disclosed to unauthorized individuals, entities or processes

- Access Controls -> Passwords, Biometric Verification, limit resource access
- Encryption -> The process of encoding information so only authorized parties can read it. If in case unauthorized party intercepts the data would not be able to interpret without the encryption key
- Secure Communication -> Use secure protocols as TLS on transfer data to prevent interception

Integrity -> Protecting data from unauthorized changes (accuracy of data)

- Data Accuracy
- Data Consistency
- Data Trustworthiness (you can trust)

Methods:

- Cryptographic hash Functions
- Digital Signatures
- Access Controls (edit permission)

Availability -> Ensure that data, systems and services are accessible to authorized users when needed

- Fault Tolerance -> Even if a component fail the system would still be accessible (multi region, cluster, HA (Active-Passive OR Active-Active)
- Backup System -> Regularly backing up data to enable recovery in case of data loss or corruption

Disclosure X Confidentiality
Alteration X Integrity
Denial X Availability