Cyber Security Fundamentals

**Information, Computer & Network Security**

Information Security refers to the protection of available information or information resources

from unauthorized access, attack, theft, or data damage. Responsible individuals and organizations must secure their confidential information.

Computer security is the protection of computer systems and information from harm, theft,

and unauthorized use. Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.

**Key Objectives of Computer Security**

Confidentiality:

Preserving authorized restrictions on information access and

disclosure, including means for protecting personal privacy and

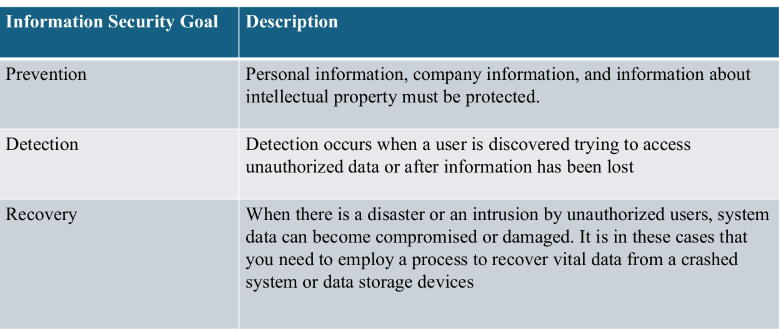
proprietary information. A loss of confidentiality is the unauthorized disclosure of information

This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

**Goal of Information Security**



**CIA Triad**

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes

referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.



