Overview of Information Security Concepts

- Information security: the protection or safeguarding of information and information systems from unauthorized access, disclosures, alterations, and destruction.
  - Can also be described as a state of well-being for information and infrastructure in which the possibilities of information and services theft, tampering, and disruption are low or tolerable.
- Information Security Elements:
  - Confidentiality: Assurance that the information is accessible only to those authorized to have access.
  - Integrity: Trustworthiness of data or resources in terms of preventing improper and unauthorized changes
  - Availability: Assurance that the systems are accessible when required by the authorized users
  - Authenticity: Characteristic of a document, communication, or dataset that ensures that it is genuine.
  - Non-Repudiation: Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- Confidentiality, Integrity, and Availability are together referred to as the CIA triad.
- Defense-In-Depth: a security strategy in which several protection layers are placed throughout an information system.
  - helps to prevent direct attacks against an information system and data as a break in one layer only leads the attacker to the next layer.

Created by: Abdelrahim Alsadiq

- Information Security Policies: the foundation of the security infrastructure that defines the basic security requirements and rules necessary to protect and secure an organization's information systems. It contains:
  - All security policies must be documented properly, and they should focus on the security of all departments in an organization.
- Technical Security Policies: describe the configuration of the technology for convenient use.
- Administrative Security Policies: address how all persons should behave.
- Types of Security Policies:
  - Promiscuous Policy: does not impose any restrictions on the usage of system resources.
  - Permissive Policy: starts from a wide-open base, and the majority of internet traffic is accepted, but known dangerous services and cyberattacks are blocked.
    - should be updated regularly to be effective.
  - Prudent Policy: starts with all services blocked, and the administrator enables safe and necessary services individually.
  - Paranoid Policy: forbids everything. There is a strict restriction on all use of company computers, whether it is system usage or network usage. There is either no internet connection or severely limited internet usage.