Date: 12th September 2024

Mentor: Risala Mam

**Key objectives :**

1. Confidentiality

* Data confidentiality
* Privacy

1. Integrity

* Data integrity
* System integrity

1. Availability

**Goals :**

1. Prevention
2. Detection
3. Recovery

**Security management process:**

1. Identify security controls. NIDS (network intrusion detection system)
2. Implement security controls (previous incident wise) IDS(intrusion detection system), IPS(intrusion prevention system)
3. Monitoring security control (anti-virus notifications)

**### CIA Triad :** confidentiality , Integrity ,Availability after authentication  + authenticity , accountability

**Basic Concepts:**

1. Vulnerabilities
2. Threats
3. Risk= likelihood \* impact , 1\*2
4. Attacks (physical, software based , social engineering, web app based , network based)
5. Security control  (Prevention, detection, recovery)

Identity , authentication, authorization

Accounting and auditing : parts of accounting in which a security professional examines logs of what was recorded.

**Least privilege model :**

**DAD :** disclosure, alteration, denial

Data Loss Prevention :

**Data classification:**

1. Personally identifiable information
2. Personal data
3. Sensitive personal info
4. Non-public personal info

**Data security state** :

1. At rest
2. In transit
3. In use

OSI security attack:

Attack , mechanism, service

**Attacks :**

* passive attacks : release of message contents and traffic analysis(sniffing)
* Active attacks :

1. Masquerade
2. Denial of services
3. Modification
4. Replay

**Geolocation:** Authentication according to location