**Principles of Security**

1. **Introduction:**

* Defense In Depth

1. **The CIA Triad:**

* Confidentiality
* Integrity
* Availability

1. **Principles of Privileges:**

* The levels of access given to individuals are determined on 2 factors:
  + The individual's role/function within the organization
  + The sensitivity of the information being stored on the system
* Privileged Identity Management (PIM)
* Privileged Access Management (PAM)
* Principle of least privilege

1. **Security Models Continued:**

* The Bell-La Padula Model (Confidentiality| Can’t read up, can read down)
  + Vetting
* Biba Model (Integrity| Can read up, can't read down)
* “No write down, No read up” RULE

1. **Threat Modelling & Incident Response:**

* Threat Modelling Process
  + Preparation
* Incident Response (IR)
* Urgency & Impact Classification
* CSIRT (Computer Security Incident Response Team)
* Six Phases of Incident Response
  + Preparation
  + Identification
  + Containment
  + Eradication
  + Recovery
  + Lessons Learned
  + Identification
  + Mitigations
  + Review
* Effective Threat Model
  + Threat intelligence
  + Asset identification
  + Mitigation capabilities
  + Risk assessment
* STRIDE
  + Spoofing identity
  + Tampering with data
  + Repudiation threats
  + Information disclosure
  + Denial of Service
  + Elevation of privileges
* PASTA (Process for Attack Simulation and Threat Analysis)