# Protecting Security of Assets

1. Classifying and Labeling Assets
    - One of the first steps in asset security is classifying and labeling assets.
    - Protected Health Information
    - Proprietary Data
        - Proprietary data refers to any data that helps an organization maintain a competitive edge.It could be software code it developed, technical plans for products, internal processes, intellectual property, or trade secrets.
        - Defining Classifications
            - Top Secret
            - Secret
            - Confidential
            - Unclassified
    - Defining Data Security Requirements
        - After defining data classifications, it's important to define the security requirements.
    - Understanding Data States
        - Data at Rest
        - Data in transit
        - Data in use
    - A key goal of managing sensitive data is to prevent data breaches.
    - Marking Sensitive Data
    - Marking also includes using digital marks or labels.
    - Handling Sensitive Data
        - Handling refers to the secure transportation of media through its lifetime.
        - Policies and procedures need to be in place to ensure that people understand how to handle sensitive data.
    - Storing Sensitive Data
        - Sensitive data should be stored in such a way that it is protected against any type of loss.
    - Destroying Sensitive Data
        - Data remanence is the data that remains on a hard drive as residual magnetic flux.
        - A degausser generates a heavy magnetic field, which realigns the magnetic fields in magnetic media
        - The following list includes some of the common terms associated with destroying data:
            - Clearing
            - Erasing
            - Purging
            - Declassification
            - Sanitization
            - Degaussing

- Destruction
- Degaussing and Purging is very important

2. Identifying Data Roles
    - The data owner is the person who has ultimate organizational responsibility for data.
    - The system owner is the person who owns the system that processes sensitive data
    - The system owner is responsible for ensuring that data processed on the system remains secure.
    - A data administrator is responsible for granting appropriate access to personnel.
    - Data owners often delegate day-to-day tasks to a custodian.
3. Protecting Privacy
    - Many laws require organizations to disclose what data they collect, why they collect it, and how they plan to use the information.
    - Baselines provide a starting point and ensure a minimum security standard.
    - Scoping refers to reviewing baseline security controls and selecting only those controls that apply to the IT system you're trying to protect.