

Asset Security | Ivan Notes 2022

▼ 1. Create & maintain Asset Inventory

- Assign ownership

▼ 2. Classify - based on value

- ▼ data classification policy
 - standards, procedures, baselines, guidelines
- ▼ classification
 - ▼ labeling
 - e.g. Public, secret, top secret
 - ▼ marking
 - how it should be protected
- categorization

▼ 3. Protect - based on classification

- ▼ Roles
 - ▼ data owner/controller
 - accountable for data
 - ▼ data processor
 - e.g. CSP
 - ▼ data custodian
 - technical aspects of the data
 - ▼ data steward
 - governance and compliance
 - ▼ data subject
 - who/what the data is about
- ▼ at Rest
 - encryption
 - access control
- backups

- ▼ Motion
 - end to end encryption, only decrypted once it reaches destination
 - link encryption - decrypted and reencrypted at every node
 - onion networks, e.g. TOR
- ▼ in Use
 - homomorphic encryption
- Archive
- ▼ **4. Defensible destruction**
 - ▼ physical destruction
 - media destruction
 - shred / disintegrate / drill
 - degauss
 - ▼ purging
 - degauss
 - crypto shredding
 - ▼ clearing
 - overwrite / wipe / erasure
 - format
- **5. Assess & Review**
- ▼ **Privacy: state or condition of being free from being observed or disturbed by other people**
 - ▼ Privacy policy
 - standards, procedures, baselines, guidelines
 - ▼ Personal data
 - PII, SPI, PHI, PI
 - Direct identities
 - ▼ indirect identities
 - age, gender, ethnicity
 - online identities
 - ▼ Information lifecycle

- create / update
- store
- use
- share
- archive
- destroy
- ▼ OECD guidelines
 - collection limitation
 - data quality
 - purpose specification
 - use limitation
 - security safeguards
 - openness
 - individual participation
 - accountability
- ▼ GDPR
 - supervisory authority (SA)
 - Core of EU privacy regulation, many countries model after this
- Cannot achieve privacy without security