

Domain 2: Asset Security

Index

Asset Types	3
Asset Classification	3
Asset Storage	3
Asset Security	3
Data Classification	3
Type of Data	4
Data Stakeholders	4
Data Remanence	4
Data Destruction	4
Scoping	4
Tailoring	4
Tokenization	4
Anonymization	4
Data Security	5
Digital Rights management	5
DRM license	5
Cloud Access Security Broker (CASB)	5
Data Loss Prevention (DLP)	5

Asset Types

- Tangible - anything you can physically touch. For e.g.: Laptops, Buildings
- Intangible - anything of value that you can't physically touch. For e.g.:
 - Trademarks
 - Trade Secrets
 - Copyrights
 - Patents

Asset Classification

- Personally Identifiable Information - Can be used to distinguish an individual's identity
- Personal Health Information - Processed by health organizations, schools, employer
- SPI

Asset Storage

Apply appropriate controls based on classification

- Encryption - AES256
- Physical Security
 - Safes
 - Secure Rooms
 - Cabinets
 - HVAC

Data is more valuable than the media

- Buy high quality media
- Buy media with built-in security

Asset Security

- EOL - OEM will no longer manufacture a particular product
- EOS - OEM will no longer provide service to a particular product

Data Classification

- Confidential - Disclosure = damage
- Top Secret - Disclosure = exceptionally grave damage
- Secret - Disclosure = serious damage
- Private - Disclosure = grave damage
- Public - Disclosure = no damage

Type of Data

- Data at rest - Stored on media. E.g. data stored in hard drive
 - Controls - Symmetric Encryption
- Data at motion - Moving across a network
 - Controls - Transport Encryption
- Data in use - Data in temporary storage buffer while being used
 - Controls - Purging after use

Data Stakeholders

- Business Owner - Senior executive that makes policy to govern data security
- Data Owners - Management level who owns the data
- Data Custodians - Technical people who do configurations
- System Owner - Person who owns the hardware where data is kept

Data Remanence

Data left over after a removal and deletion process

Data Destruction

- Shredding - Shred to 2 mm
- Degaussing - Degaussing don't work on SSD
- Overwriting
- Purging

Scoping

Portion of standards that will be applicable for organization

Tailoring

Customizing standards as per the organization's need.

Tokenization

Using random string of characters in place of actual data

Anonymization

Process of removing all relevant data so that it is theoretically impossible to identify the original subject

Data Security

Digital Rights management

Protects copyright data by:

DRM license

- License grants access to product and terms of use
- Contains decryption key to access the product
- Used for: Music, books, etc.

Cloud Access Security Broker (CASB)

Sits between cloud app users and cloud services to control access.

- Network Based - Intercepts traffic to monitor and take actions
- API Based - Blocks unauthorized queries via API

Data Loss Prevention (DLP)

Works using various mechanisms:

- Pattern matching - Detects specific regular expressions and takes action as per the defined rule
- Keyword based - Detects specific keyword like SPI, PII, etc. and block the communication
- Network Based - Restrict email and other network sharing mechanisms
- Endpoint based - Restricts copy and printing of data