

Compliance and Assessment

Domain 5.0

The Importance of Data Privacy and Protection

Chapter 19

Episode 19.01

Data Privacy and Security

Objective: 5.1 Understand the importance of data privacy and protection.

- Privacy vs. security

Data Privacy and Security

- Privacy vs. security
 - Privacy is about the individual
 - Security is about the data
- Privacy vs. confidentiality
 - Confidentiality is about the data
 - Privacy is about keeping an individual's identity secure
- Data security is protected through controls
- Privacy has to do with data usage

Data Privacy and Security

- Types of data
 - Personal
 - Personal health
 - Financial
 - Copyrighted
- Legal requirements for data
 - GDPR
 - HIPAA
 - US copyright law
 - PCI DSS

Episode 19.02

Nontechnical Controls

Objective: 5.1 Understand the importance of data privacy and protection.

- Non-technical controls
 - Classification
 - Ownership
 - Retention
 - Data types
 - Retention standards
 - Confidentiality
 - Legal requirements
 - Data sovereignty
 - Data minimization
 - Purpose limitation
 - Non-disclosure agreement (NDA)

Nontechnical Controls

- Data ownership
- Data classification
- Data confidentiality
 - Nondisclosure agreement (NDA)
- Data sovereignty
 - Principle behind GDPR
- Data minimization
- Data purpose limitation

Data Retention

- Standards
 - What data do we keep?
 - How long do we keep this data?
 - Where do we keep this data?
 - How do we delete data?

Data Retention

- Taxonomy
 - How data is stored and organized for future recall
- Normalization
 - Makes it possible to relate data and extract meaningful reports
- Indexing
 - Way of organizing data for searchability and rapid recall

Episode 19.03

Technical Controls

Objective: 5.1 Understand the importance of data privacy and protection.

- Technical controls
 - Encryption
 - Data loss prevention (DLP)
 - Data masking
 - Deidentification
 - Tokenization
 - Digital rights management (DRM)
 - Watermarking
 - Geographic access requirements
 - Access controls

Technical Controls

- Access controls
 - Limit access to certain resources
 - Identification, authentication, authorization
- Encryption
 - Protects confidentiality
- Sharing data while preserving privacy
 - Data masking
 - Deidentification
 - Tokenization

Technical Controls

- Digital rights management (DRM)
 - Watermarking
 - Geographic access requirements
 - Geoblocking

Technical Controls

- Data loss prevention (DLP)
 - Process:
 - Create data inventories
 - Monitor data flows
 - Implement, test, tune
 - DLP solution placement
 - Network DLP (NDLP)
 - Endpoint DLP
 - Hybrid DLP