



SEC+

Lesson 16:

Summarize Data Protection and Compliance Concepts

Lesson 16

Topic 16A

Data Classification and Compliance

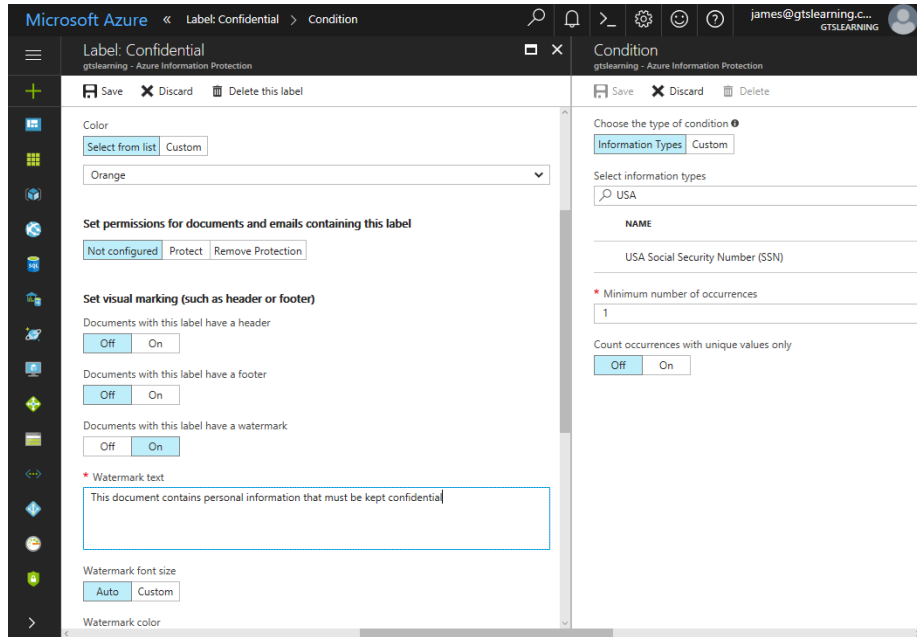


Data Types

- Categorizing or classifying data based on its inherent characteristics, structure, and intended use
- Regulated Data
- Trade Secrets
- Intellectual Property
- Legal and Financial Data
- Many Others

Data Classifications

- Identifying the importance and associated protections required to protect different types of data
- Typically defined in 3 levels



Using Microsoft Azure Information Protection to define an automatic document labeling and watermarking policy. (Screenshot used with permission from Microsoft.)

Data Sovereignty and Geographical Considerations

- Data Sovereignty
 - A legal jurisdiction restricting processing and storage of data on systems that do not physically reside within that jurisdiction
- Geographical Considerations
 - Organizations must ensure data remains within a designated boundary
 - Access controls to validate a user's geographic location

Privacy Data

- Personally identifiable or sensitive information associated with an individual's personal, financial, or social identity
- Data that could infringe upon an individual's privacy rights, if exposed or mishandled
- Data protection and privacy laws safeguard both data types
 - Rapidly evolving legal environment
- Privacy data is closely associated with the rights of individuals to control the use and disclosure of their personal information
- Individuals have the right to access, correct, and request the deletion of their privacy data

Privacy Data

- Legal Implications
 - Protecting privacy data carries significant local, national, and global legal implications
 - Many countries have specific privacy laws and regulations that dictate how personal data should be handled within their jurisdiction
 - The General Data Protection Regulation (GDPR) in the European Union has had a substantial impact globally by setting high privacy and data protection standards
 - GDPR applies to organizations that process the personal data of EU residents, regardless of their physical location
- Roles and Responsibilities
 - Data Controller and Data Processor
 - Both roles are responsible for ensuring personal data protection in compliance with data protection laws and regulations
 - Data Subject

Privacy Data

- Right to Be Forgotten
 - Fundamental principle outlined in the General Data Protection Regulation (GDPR)
 - Grants data subjects the right to request the deletion of their personal data under certain circumstances
- Ownership of Privacy Data
 - It is not easy to attribute traditional notions of ownership to privacy data
 - Many data protection laws place the emphasis on protecting the data subject
- Data Inventories and Retention
 - Detailed record of personal data being collected, processed, and stored
 - Retain personal data only for as long as necessary to fulfill the intended purpose or as required by law

Privacy Breaches and Data Breaches

- When information is read, modified, or deleted without authorization
- Organizational Consequences
 - Reputation damage
 - Identity theft
 - Fines
 - Intellectual Property (IP) theft
- Breach Notification
 - Requirements for different types of breach are established in laws and in regulations
 - Public Notification and Disclosure

Compliance

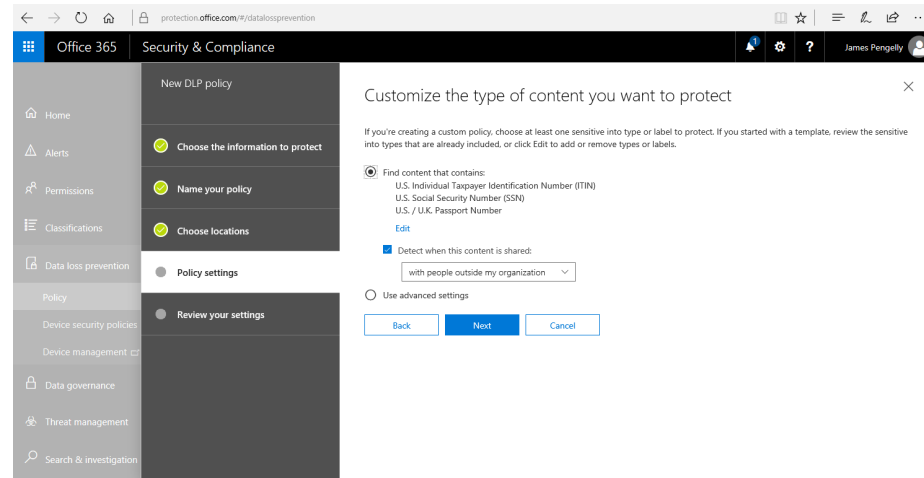
- Security compliance refers to organizations' adherence to applicable security standards, regulations, policy and best practices
- Compliance Issues
 - Legal & Regulatory Noncompliance
 - Software Licensing
 - Contractual Noncompliance

Monitoring and Reporting

- Systematically assessing, evaluating, and reporting an organization's adherence to laws, regulations, contracts, and industry standards
- Internal and External Compliance Reporting
- Compliance Monitoring

Data Protection and Data Loss Prevention

- Data requires different protection methods for each state
 - Data at rest
 - Data in motion
 - Data in use
- Data Loss Prevention
 - Automates the discovery and classification of data types and enforce rules so that data is not viewed or transferred without a proper authorization



Creating a DLP policy in Office 365. (Screenshot used with permission from Microsoft.)

Data Classification and Compliance

- Data Types
- Data Classifications
- Data Sovereignty and Geographical Considerations
- Privacy Data
- Privacy Breaches and Data Breaches
- Compliance
- Monitoring and Reporting
- Data Protection
- Data Loss Prevention

Lesson 16

Topic 16B

Personnel Policies



Conduct Policies

- Operational policies include credential management, data handling, incident response and those governing employee conduct and respect for privacy
- Acceptable Use Policy
- Code of Conduct
- Social Media Use and Analysis
- Use of Personally Owned Devices
- Clean Desk Policy

User and Role-Based Training

- Untrained users represent a serious vulnerability because they are susceptible to social engineering and malware attacks and may be careless when handling sensitive or confidential data
- Appropriate security awareness training needs to be delivered to employees at all levels, including end users, technical staff, and executives
- Training should be tailored to the audience and job role

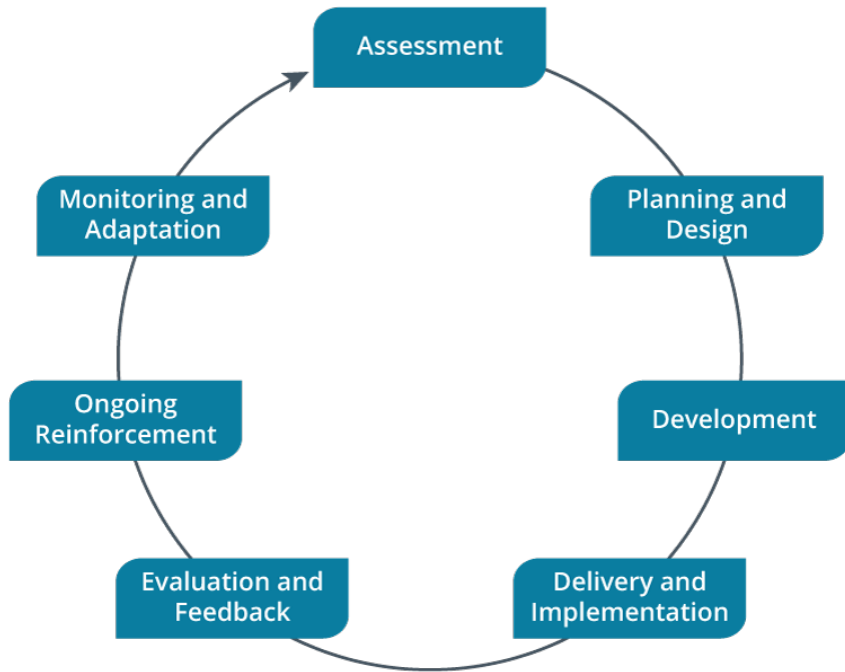
Training Topics and Techniques

- Popular Techniques
 - Computer-Based Training
 - Gamification
 - Phishing Campaigns

Training Topics and Techniques

- Topics
 - Situational Awareness
 - Reporting and Escalation Procedures
 - Policy/Handbooks
 - Insider Threat
 - Password Management
 - Removable Media and Cables
 - Hybrid/Remote Work Environments

Security Awareness Training Lifecycle



Security Awareness Training Lifecycle.

- Security awareness training practices should follow a lifecycle approach consisting of several stages

CompTIA Security+ Exam SY0-701

Lesson 16



Summary

