Lesson 16

Explaining Data Privacy and Protection Concepts

CompTIA

Topic 16A

Explain Privacy and Data Sensitivity Concepts

Syllabus Objectives Covered

- 2.1 Explain the importance of security concepts in an enterprise environment
- 5.3 Explain the importance of policies to organizational security
- 5.5 Explain privacy and sensitive data concepts in relation to security

Privacy and Sensitive Data Concepts

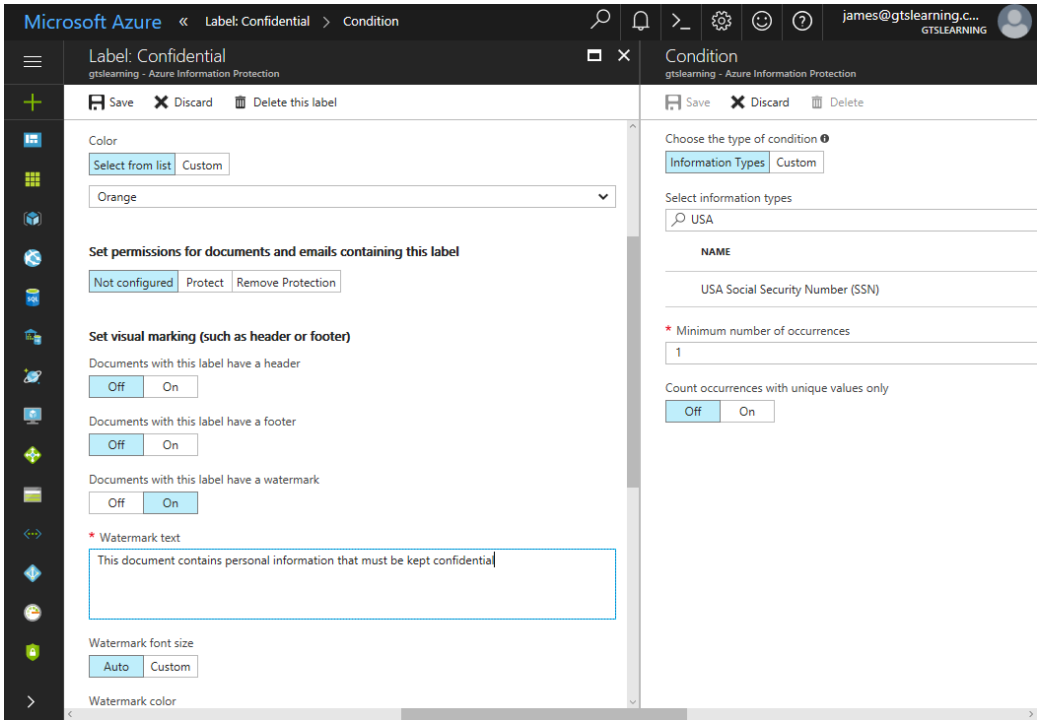
- Security
  - Confidentiality, integrity, and availability (CIA) attributes
- Privacy
  - Personal data about data subjects
  - Compliance with regulations
  - Rights of data subjects
- Information life cycle management
  - Creation/collection (classification)
  - Distribution/use
  - Retention
  - Disposal

Data Roles and Responsibilities

- Oversight and management of a range of information assets within the organization
- Data owner
  - Ultimate responsibility
- Data steward
  - Data quality and oversight
- Data custodian
  - Information systems management
- Data privacy officer (DPO)
  - Oversight of personally identifiable information (PII) assets
- Organizational roles in privacy legislation
  - Data controllers and data processors

Data Classifications

- Public (unclassified)
  - No confidentiality, but integrity and availability are important
- Confidential (secret)
  - Subject to administrative and/or technical access controls
- Critical (top-secret)
- Proprietary
  - Owned information of commercial value
- Private/personal data
  - Data that can identify an individual
- Sensitive
  - Special categories of personal data, such as beliefs, ethnic origin, or sexual orientation



Screenshot used with permission from Microsoft.

Data Types

- Personally identifiable information (PII)
  - Data that can be used to identify, contact, or locate an individual
- Customer data
  - Institutional information
  - Personal information about the customer's employees
- Health information
  - Medical and insurance records and test results
- Financial information
  - Data held about bank and investment accounts, plus information such as payroll and tax returns
- Government data
  - Legislative requirements

Privacy Notices and Data Retention

- Legislation and regulations
  - General Data Protection Regulation (GDPR)
  - Rights of data subjects
- Privacy notices
  - Purpose of collecting personal information
  - Consent to declared uses and storage
- Impact assessments
  - Assess and mitigate risks from collecting personal data
- Data retention
  - Keeping data securely to comply with policy/regulation/legislation
  - Audit requirements versus privacy requirements

Data Sovereignty and Geographical Considerations

- Data sovereignty
  - Jurisdiction that enforces personal data processing and storage regulations
- Geographical considerations
  - Select storage locations to mitigate sovereignty issues
  - Define access controls on the basis of client location

Privacy Breaches and Data Breaches

- Definition of a breach event
  - Data breach versus privacy breach
- Organizational consequences
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- Notifications of breaches
- Escalation
- Public notification and disclosure

Data Sharing and Privacy Terms of Agreement

- Service level agreement (SLA)
  - Require access controls and risk assessment to protect data
- Interconnection security agreement (ISA)
  - Requirements to interconnect federal systems with third-party systems
- Non-disclosure agreement (NDA)
  - Legal basis for protecting information assets
- Data sharing and use agreement
  - Specify terms for the way a dataset can be analyzed
  - Proscribe use of reidentification techniques

Topic 16B

Explain Privacy and Data Protection Controls

Syllabus Objectives Covered

- 2.1 Explain the importance of security concepts in an enterprise environment
- 3.2 Given a scenario, implement host or application security solutions
- 5.5 Explain privacy and sensitive data concepts in relation to security

Data Protection

- Data at rest
  - In some sort of persistent storage media
  - Encrypt the data, using techniques such as whole disk encryption, database encryption, and file- or folder-level encryption
  - Apply permissions—Access Control Lists (ACLs)—to ensure only authorized users can read or modify the data
- Data in transit (or data in motion)
  - Transmitted over a network
  - Protected by transport encryption, such as TLS or IPSec
- Data in use
  - Present in volatile memory, such as system RAM or CPU registers and cache
  - Malicious intruder with rootkit access to the computer may be able to access it
  - Trusted execution environments/enclaves

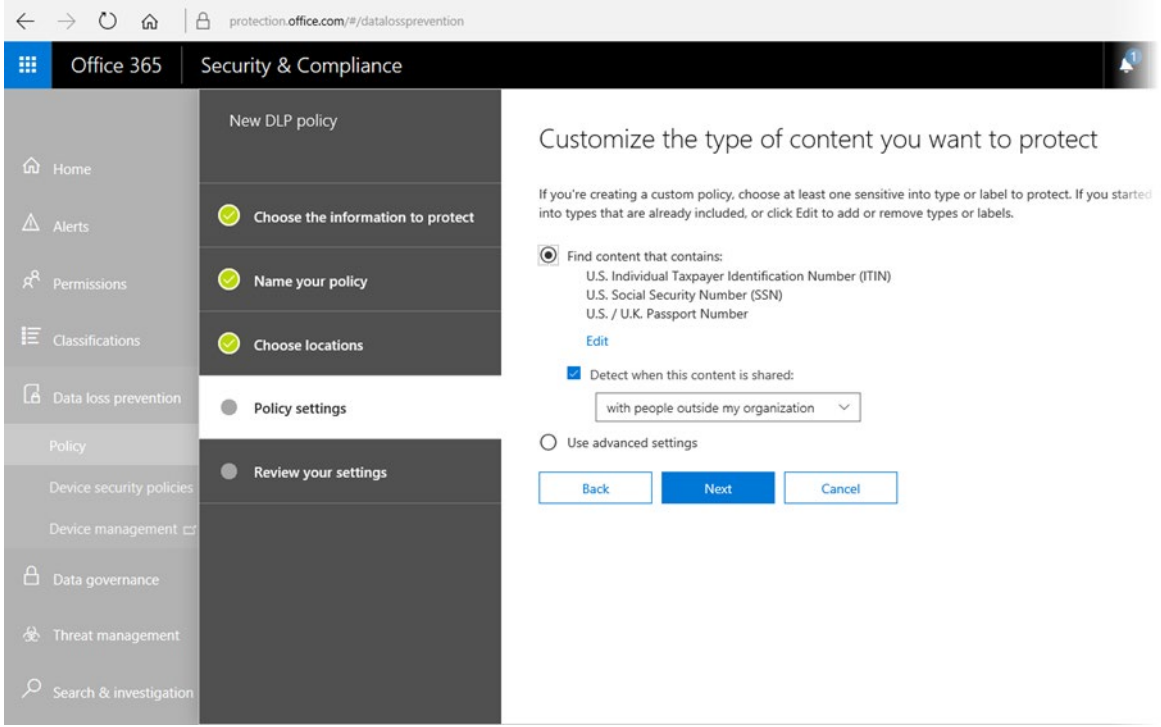
Data Exfiltration

- Data exfiltration methods
  - Removable media
  - Transferring over the network
  - Communicating data over the phone or by video
  - Taking a picture or video of text data
- Ordinary countermeasures
  - Ensure that all sensitive data is encrypted at rest
  - Create and maintain offsite backups of data
  - Ensure that systems storing or transmitting sensitive data are implementing access controls
  - Restrict the types of network channels that attackers can use
  - Train users about document confidentiality and the use of encryption to store and transmit data securely



Data Loss Prevention

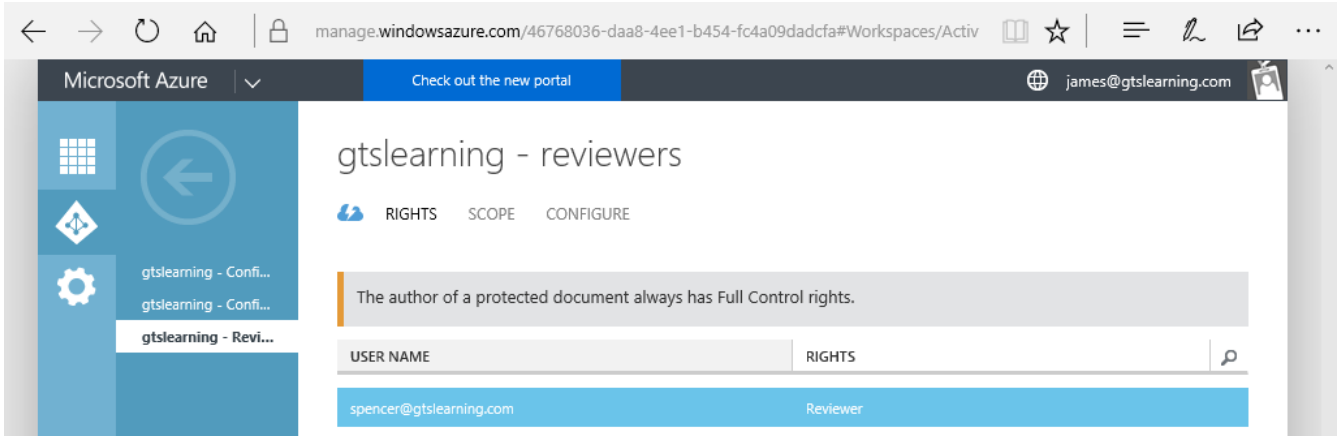
- DLP products scan files for matched strings and prevent unauthorized copying or transfer
  - Policy server
  - Endpoint agents
  - Network agents
- Cloud-based DLP
- Remediation
  - Alert only
  - Block
  - Quarantine
  - Tombstone



Screenshot used with permission from Microsoft.

Rights Management Services

- Assign file permissions for different document roles
- Restrict printing and forwarding of documents
- Restrict printing and forwarding of email messages



Screenshot used with permission from Microsoft.

Privacy Enhancing Technologies

- Data minimization
  - Only collect sufficient data to perform the specific purpose that consent was obtained for
- Deidentification
  - Removing personal information from shared data sets
- Anonymization
  - Irreversible deidentification techniques
- Pseudo-anonymization
  - Reidentification is possible using a separate data source
- Reidentification attacks
  - K-anonymous information

Database Deidentification Methods

- Data masking
  - Whole or partial redaction of strings
  - Format-preserving masks
  - Irreversible
- Tokenization
  - Replacing field value with a random token
  - Token stored in a separate data source (vault)
  - Reversible with access to the vault
- Aggregation/banding
- Hashing and salting
  - Indexing method
  - Discarding original data for identifier

Lesson 16