Identifying Sensitive Information Requirements

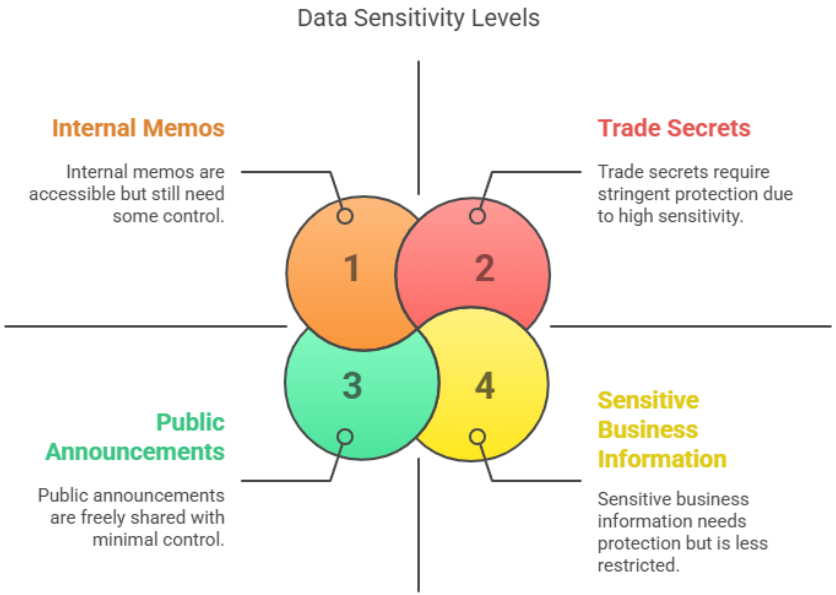
examlabpractice.com

Types of Sensitive Information

- **Personal Identifiable Information (PII):** Includes names, addresses, phone numbers, social security numbers, and any other data that can identify a specific person.
- **Financial Data:** Credit card numbers, bank account details, income, tax information, and financial records.
- **Health Information:** Protected Health Information (PHI) governed by laws like HIPAA (Health Insurance Portability and Accountability Act).
- **Intellectual Property:** Trade secrets, proprietary business information, software source code, and other confidential business data.
- **Classified Government Data:** Sensitive data that must be protected according to government regulations (e.g., FISMA, NIST guidelines).
- **Confidential Business Information:** Corporate strategies, mergers, acquisitions, legal proceedings, and other business operations.

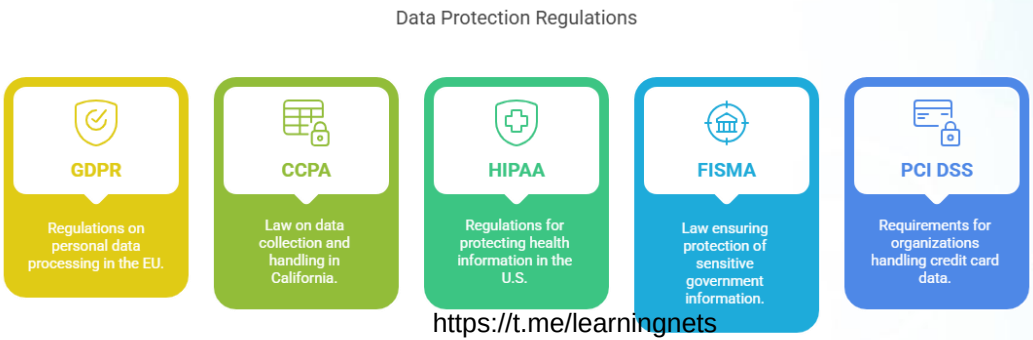
Data Sensitivity Levels

- **Public:** Can be freely shared with the public without harm to the organization.
- **Internal:** Intended for internal use only; access should be limited to employees within the organization.
- **Confidential:** Requires protection from unauthorized access, e.g., sensitive business information.
- **Highly Confidential/Restricted:** Data that, if disclosed, could cause significant harm to the organization, such as trade secrets or private health data.



Legal and Regulatory Compliance

- **GDPR (General Data Protection Regulation):** Regulations on the processing of personal data within the European Union.
- **CCPA (California Consumer Privacy Act):** Law regulating how businesses collect and handle personal data in California.
- **HIPAA (Health Insurance Portability and Accountability Act):** Regulations for protecting health information in the United States.
- **FISMA (Federal Information Security Modernization Act):** A U.S. law that ensures government agencies protect sensitive information.
- **PCI DSS (Payment Card Industry Data Security Standard):** Requirements for organizations that handle credit card information.



Tools and Techniques for Identifying Sensitive Data

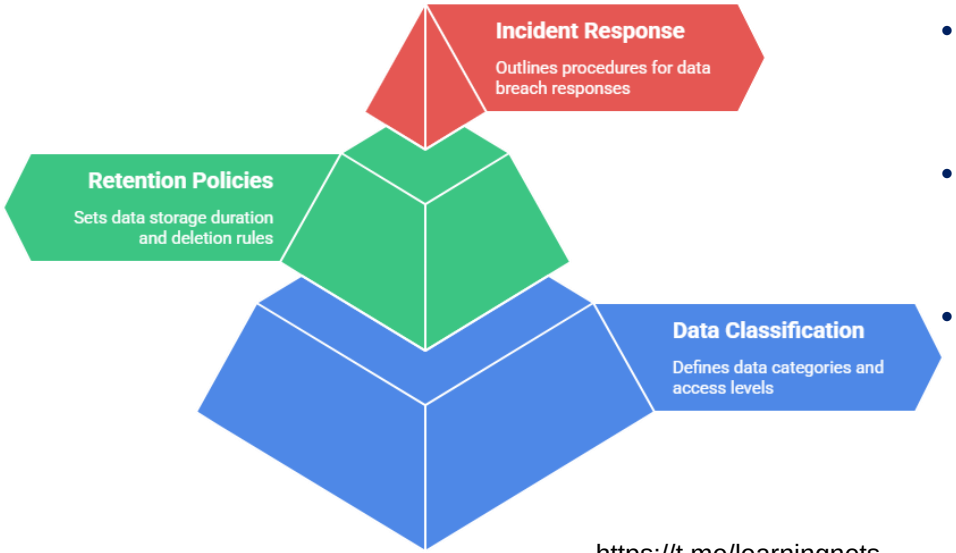
Data Classification: Labeling data based on its level of sensitivity. Organizations often have policies to help identify and classify data.

Data Loss Prevention (DLP): Technologies that help detect, monitor, and protect sensitive information from being leaked or accessed by unauthorized individuals.

Encryption: The use of encryption to protect sensitive data both at rest and in transit.

Access Control: Setting strict permissions and monitoring access to sensitive data.

Data Governance and Management Policies



- **Data Classification Policies:** Defining how data is classified and who has access to each classification level.
- **Retention Policies:** Defining how long different types of data should be kept and when they should be deleted.
- **Incident Response Plan:** A policy to respond to incidents of data breaches or leaks of sensitive information.

Assessment and Risk Management

- **Risk Assessments:** Regularly performing risk assessments to identify vulnerabilities related to sensitive data.
- **Threat Modeling:** Identifying potential threats to sensitive data and implementing security measures to mitigate these risks.