**Task:6 Data Privacy and Encryption**

**Objective:**

The objective of this task is to outline strategies for implementing data privacy and encryption within an organization. This ensures sensitive information is protected against unauthorized access and data breaches, maintaining confidentiality, integrity, and availability.

**1. Data Privacy Implementation**

Data privacy focuses on safeguarding personal and sensitive information from unauthorized access while maintaining regulatory compliance.

**Anonymization Techniques:**

1. **Tokenization of Sensitive Identifiers:**
   * Replaces sensitive data (e.g., credit card numbers) with non-sensitive tokens.
   * Original data can only be retrieved using a secure tokenization system.
2. **Pseudonymization of Personal Data:**
   * Replaces identifiable data with artificial identifiers.
   * Enables data analysis without revealing personal information.
3. **Differential Privacy for Analytical Purposes:**
   * Introduces controlled noise to datasets to protect individual privacy while allowing statistical analysis.
4. **Dynamic Data Masking:**
   * Masks sensitive information in real-time based on user roles and permissions.
   * Prevents exposure of sensitive data to unauthorized users.

**2. Encryption Strategies**

Encryption ensures that data remains confidential by converting it into an unreadable format until accessed by authorized users.

**Data at Rest:**

1. **AES-256 Encryption:**
   * Industry-standard encryption algorithm for securing stored data.
   * Provides strong security against brute-force attacks.
2. **Column-Level Encryption for Sensitive Fields:**
   * Encrypts specific database columns containing sensitive data.
   * Reduces encryption overhead while securing critical information.
3. **Full Disk Encryption:**
   * Encrypts entire storage devices, including system files.
   * Protects data even if physical devices are lost or stolen.

**Data in Transit:**

1. **TLS 1.3 Encryption:**
   * Encrypts data transmitted over networks.
   * Provides protection against eavesdropping and man-in-the-middle attacks.
2. **Secure VPN for Remote Access:**
   * Encrypts data between remote devices and the organization’s network.
   * Ensures secure access for remote employees.
3. **End-to-End Encryption for Digital Banking:**
   * Encrypts data from sender to recipient, preventing intermediaries from accessing it.
   * Critical for secure online transactions and digital banking.

**Conclusion:**

Implementing effective data privacy and encryption measures ensures sensitive information remains protected, enabling organizations to meet regulatory requirements and safeguard customer trust. These strategies help mitigate risks associated with data breaches, cyberattacks, and unauthorized access.