Exam Cram Notes: Data Protection Strategies

1. Overview

Data protection involves implementing security measures to ensure **confidentiality, integrity, and availability (CIA)** of data. This includes encryption, access controls, data loss prevention (DLP), and secure storage practices.

---

2. Data Classification & Handling

A. Data Classification Levels

✅ **Public –** No risk if exposed (e.g., marketing materials).
✅ **Internal Use –** Limited distribution within the organization.
✅ **Confidential** – Sensitive data requiring controlled access (e.g., employee records).
✅ **Restricted/Highly Confidential** – Critical data (e.g., trade secrets, financial data).

B. Data Labeling & Handling

✅ **Metadata Tags** – Identify data sensitivity and retention policies.
✅ **Data Masking –** Obscures sensitive data for non-privileged users.
✅ **Data Tokenization –** Replaces sensitive data with a non-sensitive equivalent.

---

3. Encryption & Data Security Controls

A. Data Encryption

✅ **Data at Rest –** Full Disk Encryption (BitLocker, FileVault), Database Encryption.
✅ **Data in Transit –** TLS, VPNs, SSH, IPSec for secure communications.
✅ **Data in Use –** Homomorphic encryption (for processing encrypted data).

B. Cryptographic Protocols

✅ **AES-256 (Advanced Encryption Standard) –** Strong encryption for files and databases.
✅ **TLS 1.3 (Transport Layer Security) –** Encrypts web traffic.
✅ **IPSec** – Encrypts network traffic between devices.

---

4. Access Controls & Data Governance

A. Access Control Models

✅ **Mandatory Access Control (MAC)** – Admin-defined access; common in military/government.
✅ **Role-Based Access Control (RBAC)** – Access based on job roles.
✅ **Attribute-Based Access Control (ABAC)** – Access based on attributes (e.g., location, device type).

B. Principle of Least Privilege (PoLP)

✅ **Users get only the minimum access necessary** to perform their tasks.
✅ **Just-in-Time (JIT) Privileges** – Temporary admin access when required.

C. Data Governance Policies

✅ **Data Retention Policies** – Define how long data is stored.
✅ **Data Disposal Policies** – Securely delete sensitive data (shredding, wiping).

---

5. Data Loss Prevention (DLP)

A. DLP Mechanisms

✅ **Network DLP** – Monitors & blocks unauthorized data transfers over email or web.
✅ **Endpoint DLP** – Prevents sensitive data from being copied to USB drives.
✅ **Cloud DLP** – Protects data in SaaS applications and cloud storage.

B. Insider Threat Protection

✅ **Monitor User Activity** – Track unusual file access.
✅ **Behavior Analytics** – Detects data exfiltration attempts.

---

6. Backup & Recovery Strategies

A. Backup Types

✅ **Full Backup** – Copies all data (longest time, most storage).
✅ **Incremental Backup** – Backs up only changed files since the last backup.
✅ **Differential Backup** – Backs up all changes since the last full backup.

B. Backup Locations

✅ **On-Premises** – Faster recovery but vulnerable to disasters.
✅ **Cloud Backups** – Remote storage with redundancy.
✅ **Air-Gapped Backups** – Physically isolated backups (ransomware protection).

C. Disaster Recovery (DR) Strategies

✅ **Cold, Warm, Hot Sites –** Different levels of disaster recovery preparedness.
✅ **RTO (Recovery Time Objective) –** Acceptable downtime before services must be restored.
✅ **RPO (Recovery Point Objective) –** Maximum data loss acceptable in an incident.

---

7. Secure Data Disposal

✅ **Data Wiping (Software-Based Erasure) –** Overwrites data multiple times.
✅ **Degaussing –** Disrupts magnetic storage (HDDs, tapes).
✅ **Physical Destruction –** Shredding or incineration of media.

---

8. Key Exam Takeaways

✅ **Classify data (public, internal, confidential, restricted) for security policies.**
✅ **Use encryption (AES, TLS, IPSec) to protect data at rest, in transit, and in use.**
✅ **Apply access controls (RBAC, MAC, ABAC) with least privilege principles.**
✅ **Implement DLP solutions to prevent unauthorized data transfers.**
✅ **Ensure regular, secure backups (full, incremental, differential) with recovery strategies.**
✅ **Securely dispose of sensitive data using wiping, degaussing, or destruction.**