Introduction

Purpose

The purpose of this Data Loss Prevention (DLP) Policy is to safeguard sensitive, confidential, and proprietary data from unauthorized access, use, disclosure, or loss. This policy outlines the guidelines, roles, and controls in place to prevent data breaches and ensure regulatory compliance.

Scope

This policy applies to all employees, contractors, vendors, and third-party users who have access to the organization's data. It covers all forms of data, including but not limited to digital files, emails, printed documents, and verbal communications, across all corporate systems, devices, and networks.

Roles and responsibilities

- ➔ Chief Information Security Officer (CISO)
  - Oversees the implementation and management of the DLP program.
  - Approves DLP strategies and tools.
  - Ensures alignment with legal, regulatory, and industry requirements.

- ➔ IT Security Team
  - Implements DLP technologies and monitors data flow.
  - Investigates and responds to DLP alerts and incidents.
  - Conducts periodic audits and assessments.

- ➔ Department Managers
  - Ensure staff are trained and compliant with the DLP policy.
  - Enforce DLP practices within their departments.
  - Report any data handling risks or incidents.

- ➔ Employees and Users
  - Follow DLP policies and procedures.
  - Report any suspicious activities or data security incidents.
  - Participate in required training sessions.

Prevention Controls

Technical Controls

1. Endpoint Protection
    1. DLP Agents are installed on all company-issued laptops and desktops.
    2. Personal mobile devices (BYOD) must enroll in Mobile Device Management (MDM) to access corporate data.
    3. Block or monitor file transfers to external devices (e.g., USB drives, personal cloud storage).
    4. DLP Software installed across endpoints, email systems, cloud platforms, and network perimeters is to detect, alert, or block unauthorized data movement.
2. Email and Messaging Security
    a. Scanning of outbound emails for sensitive keywords or patterns (e.g., credit card numbers, PII).
    b. Auto-encryption or quarantine of risky outbound emails.
    c. Disabling auto-forwarding to personal emails.
3. Cloud and SaaS Security
    a. Monitor data flow in and out of cloud platforms (e.g., Microsoft 365, Google Workspace, Salesforce).
    b. Enforce restrictions on unauthorized app usage (Shadow IT).
4. Web and File Transfer Control
    a. Block upload of sensitive data to unauthorized web portals.
    b. Monitor and restrict file-sharing platforms (e.g., Dropbox, WeTransfer) based on business needs.

Administrative Controls

1. Data Classification: All data is labeled based on its sensitivity (e.g., Public, Internal, Confidential, Restricted).
2. Acceptable Use Policies: Outlines what users can and cannot do with company data.
3. Incident Response: Defined procedures to address suspected or confirmed data loss.
4. User Training: Annual security awareness training with focused modules on data handling and phishing threats.
5. Remote Work Guidelines: Employees working off-site must use VPNs and secure connections.
6. Access Management: Role-based access controls (RBAC) ensure users only access the necessary data.
7. Monitoring & Logging: All data transfers and user activities are logged for forensic analysis

Physical Controls

1. Controlled access to physical data storage areas.
2. Secure document disposal (e.g., shredders, secure bins).
3. Badge access to sensitive work areas.

BYOD-Specific Policy

1. Personal mobile devices must be registered and protected by a passcode and encryption.
2. Company reserves the right to remotely wipe corporate data from personal devices in case of loss, theft, or separation from the company.
3. No local storage of sensitive data on personal devices.
4. Use of company-approved apps and containerization technologies is mandatory.

Compliance & Reviews

- The organization must comply with applicable data protection regulations such as GDPR, HIPAA, CCPA, and industry-specific standards.
- The DLP policy will be reviewed at least annually or upon significant changes in business operations or legal requirements.
- Non-compliance with this policy may result in disciplinary action, including termination of employment or contracts.

Glossary & References

- **DLP**: Data Loss Prevention – A strategy to ensure sensitive data is not lost, misused, or accessed by unauthorized users.
- **Sensitive Data**: Information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.
- **Encryption**: The process of converting data into a secure format to prevent unauthorized access.
- **DLP (Data Loss Prevention):** A set of tools and processes to prevent unauthorized access, transmission, or loss of sensitive data.
- **BYOD (Bring Your Own Device):** The practice of employees using their personal devices to access corporate systems and data.
- **PII (Personally Identifiable Information):** Information that can identify an individual, such as name, address, or ID number.
- **MDM (Mobile Device Management):** Technology used to manage and secure mobile devices accessing corporate data.

References:

ISO/IEC 27001: Information Security Management
NIST SP 800-53: Security and Privacy Controls
General Data Protection Regulation (GDPR)
Health Insurance Portability and Accountability Act (HIPAA)