Creating Cybersecurity Policies: Data Loss Prevention (DLP) Policy

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

February 14, 2025

Assignment:

(1) Choose an industry/large organization.

(2) Create a Cybersecurity Policy with the help of Artificial Intelligence (AI).

(3) **Tools and Sources Used:** ChatGPT and Grok 2.

Data Loss Prevention (DLP) Policy

EverBank

Effective Date: [Insert Date]

1. Purpose

This data Loss Prevention (DLP) policy protects EverBank's sensitive financial data from unauthorized access, transmission, or disclosure. It ensures compliance with regulatory requirements and industry standards while safeguarding customer and business information.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and anyone with access to EverBank's systems, networks, and sensitive data. It covers all forms of data, including electronic, printed, and verbal communication.

This includes but is not limited to:

- Personal Identifiable Information (PII)
- Financial information
- Customer account details
- Transactional data
- Intellectual property

3. Definitions

- **Sensitive Data**: Includes customer financial information, personally identifiable information (PII), payment card data, transaction records, and proprietary business information.
- **Data Loss Prevention (DLP) Tools**: Software solutions used to monitor, detect, and prevent unauthorized data transfers.
- **Encryption**: A security measure that converts data into a secure format to prevent unauthorized access.
- **Access Controls**: Mechanisms that restrict access to sensitive data based on user roles and responsibilities.

4. Data Classification

EverBank classifies data into the following categories:

- **Public**: Data that can be freely shared with the public.
- **Internal Use Only**: Data restricted to employees and authorized personnel.
- **Confidential**: Sensitive business information that requires limited access.
- **Restricted**: Highly sensitive data, including customer financial information, personally identifiable information (PII), and proprietary banking data.

5. Roles and Responsibilities

5.1. Employees and Contractors

- Adhere to data security best practices and report any potential data security risks.
- Do not share sensitive data outside authorized channels.
- Use encryption and secure channels for transmitting confidential information (e.g., HTTPS, VPNs).
- Regular training sessions on data security, recognizing phishing attempts, and proper data handling practices.
- Acknowledgment of policy by all employees and contractors upon hiring and annually thereafter.
- Periodic audits of employees and third-party practices.

5.2. IT and Security Teams

- Implement DLP tools to monitor and prevent unauthorized data transfers.
- Regularly audit access logs and data movement for anomalies.
- Provide employee training on data security and compliance.

5.3. Management and Compliance Teams

- Ensure adherence to regulatory requirements such as GLBA, PCI-DSS, and GDPR.
- Review and update the DLP policy annually.
- Enforce disciplinary actions for policy violations.

6. Data Protection Measures

- **Physical Security:** Secure physical documents in locked cabinets and ensure secure disposal of paper records.
- **Encryption**: All restricted and confidential data must be encrypted during storage and transmission.

- **Access Control**: Access to sensitive data is granted based on the principle of least privilege (PoLP).
- **Monitoring and Auditing**: Continuous monitoring of data access and transfers using DLP software. Real-time alerts for unauthorized data movements or anomalies.
- **Incident Response**: Procedures for responding to data breaches, including containment, investigation, notification, and remediation. Maintain an incident response team trained in handling data loss incidents.

7. Prohibited Activities

- Unauthorized copying, sharing, or transferring sensitive data.
- Using personal email or cloud storage for storing bank data.
- Printing or discarding confidential information without proper disposal.

8. Compliance and Enforcement

Violations of this policy will result in disciplinary action, which may include termination, legal consequences, or fines. EverBank reserves the right to audit compliance and implement corrective actions.

9. Review and Updates

This policy shall be reviewed annually or as needed to align with changes in regulations, threats, and business operations.

Approved by: [Name of the Chief Information Security Officer (CISO)] **Date:** [Insert Date]