Akhileshwar Chauhan

Procedure Paper 2

Company Policy for Removable Media

PURPOSE

The purpose of this policy is to introduce the risks associated with the use of removable media devices, such as USB thumb drives. Our company recently faced incidents that highlighted vulnerabilities related to data loss and unauthorized access to company data.

INTRODUCTION

Data storage and data mobility are the two important aspects of our organization, and they introduce the need for storage devices like USB drives, external hard drives, and memory cards. Along with the convenience these devices provide, a significant threat is introduced in the form of data loss, unauthorized access, and exposure of sensitive information. Recent incidents within the company have demonstrated vulnerabilities with handling of removable media and require addressing these problems.

This policy aims to introduce clear guidelines for the use, management, and monitoring of removable media to protect the company's intellectual property.

SCOPE

The scope of the policy applies to any employee, contractor, and third-party company in possession of company data. The policy applies to all forms of removable storage devices like thumb drives, external hard disks, memory cards, and other portable storage devices.

POLICY STATEMENT

Security risks while handling any form of removable storage device should be minimized using the following guidelines:

- Prohibited Use
    - None of the company devices should be introduced to any alien USB drives or any other removable storage devices.
    - Employees are prohibited from copying company data to removable forms of storage until approved for work.

- Approved Use
    - For business purposes, the company approved and issued removable media devices to be used only.
    - When not in use, all forms of removable media devices must be secured and stored by employees and reported immediately to the IT department in case of loss or theft.
- Encryption
    - All devices must be encrypted using BitLocker or an equivalent encryption tool to prevent unauthorized access.
- Data Access and Logging
    - All file transfers to and from any form of removable storage device must be logged by the IT department to monitor and audit data access.
    - Employees must update regularly and maintain a record of sensitive information stored on removable media.
- Secure Handling and Disposal
    - All outdated and unnecessary files must be deleted from removable media devices to maintain data retention policies.
    - When a removable media device is no longer needed, it must be wiped and destroyed according to protocols.
- Employee Awareness and Training
    - Employees should be trained periodically about the risks of removable media.
    - Any violation of this policy must be subjected to action.

TECHNICAL IMPLEMENTATION

The IT department will implement the following controls to enforce the policy:

- Group policy and security groups should restrict or allow access to USB to prevent unauthorized usage.
- Approved removable devices should be encrypted using BitLocker.
- Configure systems to log file transfers to and from removable storage devices to enable monitoring.
- Implement automated alerts in case of security violations related to removable storage devices.

POLICY COMPLIANCE AND REVIEW

An annual review of this policy should be done to ensure effective security with removable media. Employees are encouraged to report any violations of this policy to IT security.