MEMORY DRIVE USAGE POLICY
Table of Contents

OVERVIEW ........................................................................................................................................... 2
PURPOSE ............................................................................................................................................... 2
SCOPE ................................................................................................................................................ 2
RISKS OF NON-COMPLIANCE ........................................................................................................... 2
DEFINITION ........................................................................................................................................ 3
APPLICATION OF POLICY .................................................................................................................. 3
DATA CLASSIFICATION ....................................................................................................................... 4
ENFORCEMENT ................................................................................................................................. 4
DISPOSAL ........................................................................................................................................... 5
CONTROLS IN PLACE ........................................................................................................................ 5
VIRUS SCAN ........................................................................................................................................ 5
ENCRYPTION ..................................................................................................................................... 5
WARNING SCREEN ............................................................................................................................ 6
MONITORING/AUDITING ..................................................................................................................... 6
USER RESPONSIBILITY ...................................................................................................................... 7
CONSEQUENCES OF NON-COMPLIANCE .......................................................................................... 8
POLICY GOVERNANCE ...................................................................................................................... 8
CONCLUSION ..................................................................................................................................... 8
OVERVIEW

Dunder Mifflin, Inc. is one of the leading paper providers in the mid-Atlantic region located in Scranton, PA. Our main goal is to provide a seamless customer experience for every one of our clients. By implementing our Memory Drive Usage Policy, we can insure that our customer’s data stays safe within our network.

Our Memory Drives are meant to be used with Dunder Mifflin data only. Any removable media that contains data from our computers besides memory drives also apply. Not abiding by these policies could result in leakage of data to undesirable sources. All employees are trained to abide by these policies in full.

All employees must read and follow these policies in a way that supports the security and safety of our customers.

The CIO along with our auditing firm reviews this policy annually.

PURPOSE

This document contains the Memory Drive and Removable Media policy for Dunder Mifflin, Inc. This policy states the workplace practices and ethics that are to be used by all users for data to be safely stored and transmitted through removable media.

This policy strives to manage removable media in order to:

- Allow data to be available when required
- Maintain integrity of data
- Build confidence in data being exchanged between system
- Build trust with clients ensuring them that data is exchanged safely

SCOPE

This policy applies to all employees or anyone that intends to store data that has been provided in any way from company-owned computers.

RISKS OF NON-COMPLIANCE

Dunder Mifflin has acknowledged that risks will arise when handling removable media for business purposes. The information contained in removable media is shared throughout the organization as well as with other members outside of the organization. Any loss of customer data or interference with its integrity could significantly affect the reputation and integrity of the company. Therefore, it is imperative that the uniform implementations of these policies are maintained.
By implementing this policy, we attempt to diminish the following risks:

- Theft of protected and classified data through the careless use of the removable device
- Malware and virus infection of the network through the transfer of data by the removable device
- Legal action that could result from the release of sensitive information as a result of information leakage
- Irreparable damage of the company’s image from loss or misuse of devices

**DEFINITION**

In order to allow all employees to adhere to our policy we must provide the definition of what Dunder Mifflin considers removable (memory drive) devices.

Removable (memory drive) devices include and are not limited to:

- CDs or Optical Disks
- External Hard Drives
- USB Memory Drives
- Media Cards (SD, microSD, etc.)
- SIM Cards and Smartphones
- iPods or other Music Devices

**APPLICATION OF POLICY**

Removable devices pose potential risks to Dunder Mifflin, Inc. including the loss of information and the introduction of malware into our systems and networks. As part of our on-going efforts to protect information, systems and networks, security policy requires the following:

- Only Dunder Mifflin owned removable media devices can be connected with or plugged into a Dunder Mifflin desktop, laptop, tablet, server or other computing asset.
- Use of Dunder Mifflin owned removable media devices are restricted to authorized business purposes only.
- Any storage of Dunder Mifflin information on a removable media device must comply with policies. This includes encrypting the information to be stored on the removable media device, if the information is classified as “Confidential” or higher.
- When you store Dunder Mifflin information on removable media, you are responsible for protecting that removable media device against loss, misuse or unauthorized disclosure at all times.
- You may not use a removable media device to install, execute or use unauthorized software.
DATA CLASSIFICATION

Dunder Mifflin has established 3 classifications to describe levels of confidentiality afforded to information: “Public”, “Private”, and “Confidential”.

- **“Public”** data is information that is publicly known or available without restriction.
- **“Private”** information is data that Dunder Mifflin does not wish to be publicly disclosed, but is protected only through company policy.
- **“Confidential”** information is data that Dunder Mifflin considers significantly sensitive to require a set of controls in order to protect the data.

ENFORCEMENT

The following controls are in place to enforce the policy to protect information classified as “Private” or “Confidential” data.

- In the case of Dunder Mifflin data stored on laptops, smartphones, tablets, or similar portable computing devices, those devices must be Dunder Mifflin approved and meet the encryption standards set by the IT Services Team.
- Authentication required prior to access to Dunder Mifflin confidential data stored in a system, application or database and logging of access to the system, application or database also required during access.
- When Dunder Mifflin confidential data is stored on portable media, such as DVD, CD, magnetic tape, removable hard drives, universal serial bus (USB) drives or similar portable storage, such storage must meet the requirements of Encryption and Encryption Key Management Standards. To ensure adherence to Dunder Mifflin’s encryption standards, it is required that the IT Services Team at Dunder Mifflin, Inc. encrypts all removable media devices.
- Dunder Mifflin Confidential data must be protected against casual, unintended viewing.

PROCUREMENT

All removable media devices and any associated equipment and software must only be purchased and installed by the IT Services Team at Dunder Mifflin, except where alternative arrangements are made in writing by the head of the IT department of Dunder Mifflin. A Procurement Request Ticket (PRT) must be submitted when ordering removable media devices. This process will ensure the ordering and configuring of authorized removable media devices according to aforementioned standards listed in this policy.
DISPOSAL

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data breaches. Secure erasure of Dunder Mifflin Confidential information must be confirmed in the following situations:

- When removable media is reclaimed or disposed
- When removable media is repurposed for use in a new group
- When removable media is sent out for third party repair

Erasure must comply with minimum standards set by Dunder Mifflin. To ensure adherence to Dunder Mifflin's disposal standards, it is required that all removable media devices that are damaged or no longer required must be returned to the IT Services Team for secure disposal within 48 hours.

CONTROLS IN PLACE

Dunder Mifflin Inc. implements the following controls across its organization’s IT systems and services in order to establish appropriate, authorized, and user access guide in use of memory drives and to ensure prevention of information confidentiality and protected and classified sensitive data.

Controls are in place to protect the interests of all users of Dunder Mifflin Inc.’s information and computer systems by providing a reliable, secure and safe environment for using removable devices.

VIRUS SCAN

A virus scan must be performed before use of removable devices on all computer systems in the organization. A virus scanner dialog will be automatically displayed on any corporate computers as you insert the removable devices. Cancelling the virus scanner will prevent you from accessing the files from removable devices.

ENCRYPTION

Removable devices must be encrypted by the Dunder Mifflin Inc.’s IT Services Team in order to abide to the policy. Except for IT employees and contractors, regular employees are limited to hold only ONE encrypted removable device, less than 16GB. Memory devices will be provided to Dunder Mifflin employees upon request.
**WARNING SCREEN**

In a situation of accessing the organization’s computer systems with unencrypted memory devices, the Warning Screen will be displayed and your access information will be logged in the IT Services Team’s database as well.

The example of the Warning Screen is:

```
WARNING:
A Removable Media (USB, SD card, etc.) device has been detected

Removable Media devices pose potential risks to, including the loss of information and the introduction of malware into our systems and networks. As part of our ongoing efforts to protect information, systems and networks, security policy requires the following:

- Only Dunder Mifflin Inc. owned Removable Media devices can be connected with or plugged into a Dunder Mifflin desktop, laptop, tablet, server or other computing asset.
- Use of Dunder Mifflin Inc. owned Removable Media devices are restricted to authorized business purposes only.
- Any storage of Dunder Mifflin information on a Removable Media device must comply with policies. This includes encrypting the information to be stored on the Removable Media device, if the information is classified as “Confidential” or higher.
  IF YOU ARE UNSURE OF THE CLASSIFICATION OF THE INFORMATION, THE DATA MUST BE ENCRYPTED WHEN STORED ON THE DEVICE.
- When you store customer information on Removable Media, you are responsible for protecting that Removable Media device against loss, misuse or unauthorized disclosure at all times.
- You may not use a Removable Media device to install, execute or use unauthorized software.
```

**MONITORING/AUDITING**

IT Services Team is responsible for monitoring/populating logs of the Removable Media device at Dunder Mifflin Inc. The logs will be audited by an automated computer system biweekly in order to detect possible breaches and misuses of removable memory devices.
TRAINING

All Employees in Dunder Mifflin Inc. are required to take a number of The Removable Media drive trainings. The trainings will include 3 courses:
  1. The Removable Media Drive Policy Overview
  2. Correct Ways to Use Removable Media Drives
  3. Proper Actions to Dispose Removable Media Drives

Those trainings will help our organization to mitigate risks, provide best practices to our employees in using removable memory drives, and minimize possibility of sensitive data breach. In addition, the trainings will improve the quality of our employees’ understanding in using removable media drives, in which helping our organization to build a safe and secure information system environment.

INCIDENT MANAGEMENT

The following events, even if they are merely suspected to have occurred, must be reported to the IT Services Team within 24 hours:

- A lost, stolen, or damaged drive
- Suspected data breach
- Knowledge of misuse or negligent actions

An investigation into the case will begin immediately.

USER RESPONSIBILITY

All aspects of this policy must be followed at all times by all users for all forms of removable media drives. Extraordinary care must be taken for those media devices that are easily modifiable and transportable, which include USB flashes drives, writable CD, and writeable DVDs:

- Whenever possible, all data stored on these forms of media must be encrypted
- This equipment must be sourced from the IT Services Team. Use of personally purchased drives is not allowed.
- Even though data have been deleted, it can still be recovered. Attention must be paid to only store necessary files and documents on removable media.
- Each person must judge and take the proper care while transporting removable media in order to avoid theft, loss, or damage.
- Removable drives must only be used for the transport of files and documents. Long term storage or archiving of files must use alternative, accepted means.
- All machines with which the drive is used must have appropriate and updated virus and malware checking applications.
CONSEQUENCES OF NON-COMPLIANCE

Violations of this policy, including abuse of administrator privileges, may be cause for criminal, civil, or disciplinary action including the possibility of termination.

If any user is found to have breached this policy, they may be subject to Dunder Mifflin’s disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

POLICY GOVERNANCE

The following table identifies who within Dunder Mifflin is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person(s) who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Chief Information Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Infrastructure Manager</td>
</tr>
<tr>
<td>Consulted</td>
<td>Infrastructure Team</td>
</tr>
<tr>
<td>Informed</td>
<td>All Staff, Contractors and Partners</td>
</tr>
</tbody>
</table>

CONCLUSION

With your help we can keep our systems secure at Dunder Mifflin.