# Removable Media Policy Template

**DISCLAIMER:** This removable media policy template (USB security policy or information security policy template) is provided by [CurrentWare Inc.](http://currentware.com/) for reference purposes only.

To ensure that this policy is sufficient for your security and compliance needs it is recommended that you customize it to fit your organization’s environment and have it reviewed by key stakeholders such as executives from finance, physical security, legal, and human resources departments.

## Overview

Data loss prevention and data security are everyone’s responsibility. The very same portable nature that makes removable media devices a valued asset also introduces unique risks that must be mitigated against.

Aside from the risk of loss and theft, removable media devices are a potential source of malicious software. To help protect the sensitive data in our custody against these risks we have developed and implemented this removable media policy.

**Non-compliance with this policy may result in damages to the organization, its customers, and other stakeholders. These damages may include financial loss, a reduced ability to provide essential services, damages to the organization’s reputation, and identity theft.**

### Purpose of This Policy

This removable media policy is designed to protect the confidentiality, integrity, and availability of data when removable storage devices are used to transmit data to and from **<<ORGANIZATION NAME>>’s** systems.

This policy will operate alongside preexisting information security policies and acceptable use policies to provide guidelines and requirements regarding the security standards for the use, storage, and transportation of removable media devices and the data that is stored on them.

**The risks that this policy aims to mitigate include, but are not limited to:**

* The unauthorized disclosure or misuse of INTERNAL, CONFIDENTIAL, or RESTRICTED information (sensitive information)
* The introduction of malicious software (malware) to **<<ORGANIZATION NAME>>** networks or equipment
* Reputational risks and legal liabilities that arise as a result of data loss or the misuse of data

###

### Scope

This removable media policy applies to all employees, contractors, and any other third party conducting business with **<<ORGANIZATION NAME>>** (“Users”). This further includes all individuals and entities who use **<<ORGANIZATION NAME>>** IT facilities and equipment, or have access to, or custody of, sensitive information.

### Definitions

#### Sensitive Information

All data within the custody of **<<ORGANIZATION NAME>>** is classified as either PUBLIC, INTERNAL, CONFIDENTIAL, or RESTRICTED. **Any data that is classified as CONFIDENTIAL or RESTRICTED is considered to be sensitive information.**

* **Public Data:** Information that is openly shared and available, such as what is provided on our website. This data does not require any additional security controls.
* **Internal Data:** Organization-wide information that is solely intended for use by employees, contractors, and other representatives of **<<ORGANIZATION NAME>>**, such as employee handbooks, policies, and internal memos. As the impact of disclosure is minimal this data only needs to be protected with limited controls.
* **Confidential Data:** Sensitive organization information that must be limited to internal use only such as pricing structure, marketing materials, or non-public contact information. As the unintended disclosure of this information could negatively affect the organization, it must be protected with greater controls.
* **Restricted Data:** Information that is highly sensitive and limited to an as-needed basis, such as personally identifiable information (PII), trade secrets, and financial data. As the disclosure of this information would result in significant financial or legal impact to the organization it must be protected with significant security controls.

#### Removable Media Device

A *removable media device*—also known as a *portable storage device* or *removable storage device*—is defined as any device or media that is readable and/or writable by an end-user while being able to be moved between computers without modifications to the computer.

Removable media devices are portable devices that can be used to copy, save, store, and/or move data from one system to another.

**Examples of removable media include:**

* USB portable storage devices (“Jump Drive”, “Data Stick”, “Thumb Drive”, “Flash Drive”, etc)
* SDHC, SDXC & SD cards
* External hard drives and external solid-state drives
* R/W Compact Disk or DVD media
* Portable devices such as tablets, smart devices, and cameras
* eSATA (External Serial Advanced Technology Attachment) devices
* Floppy disks

#### Sheep Dip/Sandbox/Footbath

In a cybersecurity context, a *Sheep Dip*—also known as a *Footbath*—is a dedicated computer or sandbox environment that is used to test a removable media device for malware. A sheep-dip computer acts as the first line of defense against malware from USB drives and other portable storage mediums.

A computer that is used for sheep dipping will not be connected to the internet or the local area network; this helps prevent attackers from infiltrating the network through the sheep-dip computer and prevents the spread of computer worms.

The sheep-dip computer will be provided with an up-to-date antimalware system (virus scanner) for the purpose of scanning removable media devices for malicious software before allowing them onto a networked computer.

The term “Sheep Dip” refers to a method used by farmers to prevent the spread of parasites in a flock of sheep. During a sheep dip, farmers will dip all of their sheep one after another in a trough of pesticide to prevent infestations to the rest of their flock.

Similarly, the practice of sheep dipping removable media devices acts as an essential layer of security by preventing potentially infected storage devices from connecting to networked computers without prior inspection.

#### Data Loss/Data Leak

*Data loss* is any incident that results in data being corrupted, deleted, and/or made unreadable. A data loss event typically occurs due to intentional or accidental deletion, a malicious attack that results in data corruption, or physical damage to data storage hardware.

Similarly, a *data leak* is the unauthorized exposure of sensitive information through accidental or malicious actions. The incident could occur due to server misconfigurations, lost/stolen removable media devices, or an attack from a threat actor.

## Guiding Principles

1. Removable media devices will only be approved for use if there is a valid business use case that outweighs the associated risks and all other options to transfer data have been exhausted.
2. Only removable media devices that meet **<<ORGANIZATION NAME>>**’s security standards will be permitted on networked computers.
3. Data loss prevention is not the sole responsibility of any individual or department; it requires the cooperation and due diligence of everyone involved. All users of removable media containing sensitive information have a duty of care to protect the devices against unauthorized access, misuse, or corruption.
4. The secure use of removable media devices is just one aspect of a comprehensive information security program that must be adopted to effectively safeguard sensitive information.

## Security Responsibilities & Practices for Removable Media Devices

### Security Requirements for Removable Media Devices

#### Permitted Devices

**<<ORGANIZATION NAME>>** will ensure that all users with a requirement for removable media devices are provided with a pre-authorized device and all related assets that they will need to securely store, transport, and access data.

**Only devices that have been pre-authorized by <<ORGANIZATION NAME>> will be permitted for use.** Special exemptions may be made at the discretion of information security personnel for trusted third parties when no other data transmission options are available (see “*Managing the Security Risks of Third-Party Removable Media Devices*”).

* Personally owned devices are prohibited from use on all networks and computers.
* Organization-provided devices are not permitted to be used on personally owned devices.
* Under no circumstances should unidentifiable removable media devices be used. If an unidentifiable device is found it can be brought to information security personnel for safekeeping or secure inspection at their discretion.

#### The Sheep Dipping Process

All removable media devices must be connected to a sheep-dip computer for inspection prior to being allowed on networked computers.

To inspect the removable media device you must:

1. Log in to the sheep-dip computer
2. Insert the device(s) that will be inspected
3. **<<VIRUS SCANNING PROCESS>>**

In the event that a potential threat is discovered during the sheep-dipping process, **the device may not be connected to any other computer.** The device must be removed from the sheep-dip computer and information security personnel must be alerted immediately.

#### Managing the Security Risks of Third-Party Removable Media Devices

In the event that a critical data transfer is required from a third-party removable media device that has not been pre-authorized, that device must be connected to a sheep-dip computer for inspection prior to being allowed on networked computers.

**Removable media devices will only be allowed from third parties when…**

* There is a clear business requirement to load the data from the device to an organization-owned computer
* No suitable alternatives are available (the use of the removable media device must be a last resort)
* The sheep-dipping process does not indicate the presence of a security threat (See *“The Sheep Dipping Process”*)

If the above criteria are met, you must contact information security personnel to have the third-party device added to the Allowed Devices List or for a temporary access code to be generated for your computer.

### Responsible Use Expectations for Users

#### Duty of Care & Incident Reporting

All members and associates of **<<ORGANIZATION NAME>>** have a duty of care to protect the sensitive information in our custody.

**This duty of care mandates that:**

* All members and associates of **<<ORGANIZATION NAME>>** are expected to be in compliance with this policy and all other information security policies.
* All suspected or definitive security incidents, misuse, or irresponsible actions are to be immediately reported to **<<POINT OF CONTACT>>.**
* All members and associates of **<<ORGANIZATION NAME>>** understand and abide by their cybersecurity awareness training.
* All members and associates of **<<ORGANIZATION NAME>>** understand their responsibilities associated with the secure use of technology when it comes to protecting sensitive information while performing their duties.

#### Unauthorized Software & Executables

While removable media devices allow for the convenient transmission of executable software, all software that is used on **<<ORGANIZATION NAME>>** computers must be exclusively purchased, installed, and managed by information security personnel.

**There is a zero-tolerance policy for the use of unauthorized software (“Shadow IT”) on organization-owned equipment and systems.**

#### Physical Security Controls

Each removable media device is assigned to a designated individual. The individual is responsible for the physical protection of the removable media device and must ensure that steps are taken to protect the sensitive data on the device from loss, theft, or damage.

Under normal operating conditions, all removable media devices must be signed in and out each workday on an as-needed basis. In the event that the extended possession of a removable media device is granted, the user is responsible for meeting its ongoing security requirements.

**These steps include, but are not limited to:**

* Under no circumstances can the individual share the device with others; it must remain in their sole custody until it is returned to information security personnel.
* When not in use, any removable media device containing sensitive data must be stored securely, such as in a locked cabinet or safe.
* All removable media devices must be returned to a designated safe storage location at the end of each workday unless special authorization is provided in writing.
* Do not leave removable media devices unattended. When a transfer of sensitive data is underway the device must remain in the authorized user’s physical control at all times.

#### Data Handling Procedures for Removable Storage

##### Data Loss Prevention & Data Integrity

* Data must only be copied to a removable media device by an authorized user in the performance of their official duties or when responding to legitimate requests for information.
* Removable media devices are only to be used for the temporary storage and transmission of information. They must not be used as an alternative to other storage equipment for critical backups.
* Unless special authorization is provided in writing, under no circumstance should removable media be connected to any computer that has access to RESTRICTED data.
* CONFIDENTIAL or RESTRICTED information may not be stored on removable media without explicit permission.
* To ensure the integrity of data, all amendments made to data on removable media devices must be reflected in **<<ORGANIZATION NAME>>**’s private network at the nearest available opportunity.

##### Encryption & Authentication Requirements

* When sensitive information is stored on removable media, the device must be encrypted and password-protected to prevent unauthorized disclosure of the data. The password must be unique, difficult to guess, and not shared with any other parties.
* The encrypted removable media device must carry the same public-private key combination that is associated with the authorized user.

#### Clearing & Disposal

* All users must return their assigned removable media devices at the end of the workday unless special authorization is provided.
* All organization property must be returned at the end of the employment period, including removable media devices.
* Under no circumstances should any removable media device be given away or disposed of via any channel other than through information security personnel. Damaged or faulty devices must be brought to information security personnel for secure disposal or repair.
* Users must note that files and data that have been deleted from removable media devices can still be retrieved. Any device that once stored sensitive information must be treated as if it still contains the sensitive information until it has been securely erased by information security personnel. If full data erasure is not feasible, the USB device must be limited to the use of the highest data classification for which it was previously used; the device cannot be considered for declassification.

### Organizational Security Controls for Removable Media

In addition to the responsibilities that users have to protect sensitive data on removable media devices, **<<ORGANIZATION NAME>>** provides organizational security measures to reduce the risks associated with removable media devices.

#### Device Control Software & USB Removable Disk Auditing

All computers with access to sensitive data and/or connection to the organization’s network have USB control software installed on them.

This software protects the organization’s systems against the risks of removable media devices by:

* Preventing the loading of data from non-authorized portable storage devices
* Restricting the types of data that can be transmitted to authorized portable storage devices
* Logging all file operations to and from portable storage devices
* Logging all removable media devices that are plugged into monitored computers

Monitoring and tracking the use of removable media devices is standard practice as part of **<<ORGANIZATION NAME>>**’s asset management and cybersecurity processes.

**As a condition of using systems provided by <<ORGANIZATION NAME>>, you acknowledge that all computer activity may be monitored for security and productivity management purposes.**

#### IT Inventory Management

All departments must maintain accurate and up-to-date records of the removable media devices issued within the organization.

At a minimum, the records will contain:

* A unique identifier of the device, such as a serial number
* The name of the user the device is assigned to
* The date of assignment
* The business purpose that the device is assigned for
* The highest security classification of the information that is allowed to be stored on the device

**NOTE:** All removable media containing sensitive information must have an external label that indicates the highest data classification and the user responsible for its safekeeping.

#### Cybersecurity Awareness Training

**<<ORGANIZATION NAME>>** provides ongoing cybersecurity awareness training to promote awareness of information security policies, procedures, and best practices among its users. This training is intended to educate users on the responsibilities and risk factors associated with their role in the organization.

If at any time a user desires retraining, they can access the training materials by going to **<<TRAINING MATERIALS LOCATION>>.**

## Exceptions to This Policy

All users are expected to be in compliance with this removable media policy and all other information security policies provided by **<<ORGANIZATION NAME>>.**

Exceptions to this policy shall only be considered in unique and rare circumstances. These exceptions require the written approval of **<<ROLE>>** and will only be granted for justifiable business purposes.

All approvals for exceptions are subject to review and expiry. The written approval will indicate the period of time for which the exception is valid. Once the approval period has passed it is the responsibility of **<<ROLE>>** to reevaluate the approval for an extension.

## Enforcement of This Policy

Anyone found in violation of this policy may be subject to corrective actions up to and including the suspension of their access to technology resources, legal action, and/or dismissal.

## Acknowledgment

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Employee signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 **<<ROLE>>** signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Witness signature Date

#

## Enforce Your Removable Media Policy With CurrentWare

**You have the policy to set expectations for your users; now it’s time to enforce it.** Get started today with a free trial of CurrentWare’s device control software AccessPatrol. Want to learn more? See how Viking Yachts [saved sensitive data from an insider threat](https://www.currentware.com/customers/viking-yachts/) with AccessPatrol's USB activity reports.

### [AccessPatrol](https://www.currentware.com/accesspatrol/)

**Device Control Software**

* Prevent data theft to USB devices
* Real-time USB usage alerts
* Allow only authorized USB devices

### [BrowseControl](https://www.currentware.com/browsecontrol/)

**Web Filtering Software**

* Block websites based on URL, content category, or IP address
* Customize internet restrictions for each user, device, or department
* Schedule unique internet restrictions throughout the day

### [BrowseReporter](https://www.currentware.com/browsereporter/)

**Internet Monitoring Software**

* Get reports that show what websites are visited and how long they were browsed
* Get internet usage alerts sent straight to your inbox
* Track application usage to discover unauthorized software usage

[**Get Your Free 14-Day Trial**](http://currentware.com/download/)

**No credit card required**

CurrentWare.com | 1-888-912-9619 | info@currentware.com