Iowa County, Iowa
Policy Manual

| | |
|---|---|
| Title: Removable Media | Reference #: HR033 |
| Section: Human Resources | Date Effective/Revised: 3.10.2023 |
| Department (s): ALL | Approved By:  Board of Supervisors |

## Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

## Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Iowa County and to reduce the risk of acquiring malware infections on computers operated by Iowa County. Any questions or comments about this policy should be directed to Board of Supervisors.

## Scope

This policy covers all removable media that contains Iowa County data or that is connected to an Iowa County network.

## Policy

Iowa County staff may use removable media in their work computers. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When sensitive information is stored on removable media, it must be encrypted. Exceptions to this policy may be requested on a case-by-case basis to the Board of Supervisors.

## Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with Iowa County.

## Definitions

### Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by Iowa County.

### Encryption

Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

| | |
|---|---|
| Title: Removable Media | Reference #: HR033 |
| Section: Human Resources | Date Effective/Revised: 3.10.2023 |
| Department (s): ALL | Approved By: Board of Supervisors |

### Malware

Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.

### Iowa County Network

Being connected to an Iowa County network includes the following:

- If you have a network capable device (ex. laptop) plugged into the Iowa County Courthouse or Annex building, then you are connected to the Iowa County LAN (local area network).
- If you have a wireless capable device (ex. laptop, iPhone) and connect to the Iowa County Courthouse or Annex wireless, then you are connected to the Iowa County WLAN (wireless local area network).
- If you connect from a computer through the Iowa County Courthouse or Annex VPN (virtual private network), you are then connected to the Iowa County LAN (local area network).

### Sensitive Information

Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect Iowa County, its employees, or citizens. Examples include, but are not limited to, personal identifiers and financial information. The determination of sensitivity is the responsibility of individual departments.

| | |
|---|---|
| Title: Removable Media | Reference #: HR033 |
| Section: Human Resources | Date Effective/Revised: 3.10.2023 |
| Department (s): ALL | Approved By:  Board of Supervisors |

## Encryption Instructions

### How to encrypt a flash drive

The steps one must take to encrypt a flash drive will vary depending on what operating system your computer uses. Here's how to make it happen when you're using Windows:

1. Plug your flash drive into a USB port of your **Windows computer**.
2. Click **File Explorer**. If you can't find it, simply press the Windows logo key + E on your keyboard.
3. Right-click your flash drive and select **BitLocker**, then turn BitLocker on. BitLocker is available on supported devices running **Windows 10**, **Windows 11 Pro**, **Enterprise**, or **Education**. Next, wait for BitLocker to start.
4. Choose a password that you'll use to unlock your flash drive. It's important that you choose a strong password that others wouldn't be able to guess. Never reuse passwords across devices—your password for your flash drive should be completely new.
5. Choose how to save your recovery key. The recovery key will let you recover the information on your flash drive in case you forget the password for your flash drive.
6. Select what data you want to encrypt. You can select the entire drive or the used disk space only.
7. Click "Start Encrypting." Keep your flash drive plugged in for this entire process.
8. You'll receive a notification when the encryption process is complete. Once you receive this notification, it is safe to remove your flash drive from the computer.

### Consider a pre-encrypted flash drive

If all the above steps feel overwhelming for you, you can choose to purchase a pre-encrypted flash drive instead. When you purchase an encrypted flash drive, you'll still be required to select a password. Note that flash drives that come with encryption are generally more expensive than regular flash drives, but they can be worth it if you're trying to save yourself the headache of setting up encryption yourself.