# Removable Media Policy

**Last Update:** *February 2022*

## 1. 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.

## 2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by GP HERO and to reduce the risk of acquiring malware infections on computers operated by GP HERO. This policy is to secure and protect GP HERO, our GP Clients and their customers. GP HERO provides computer devices, networks, and other electronic information systems to provide the infrastructure for our heroes to serve our GP Customers in Australia. It is vital that GP HERO and our staff manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets both owned by GP HERO and those of our GP Clients and Customers.

## 3. Scope

This policy covers all computers and servers operating in GP HERO.

## 4. Policy

GP HERO staff may only use GP HERO removable media in their work computers. GP HEROremovable media may not be connected to or used in computers that are not owned or leased by the GP HERO without explicit permission of the GP HERO InfoSec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the GP HERO Acceptable Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by GP HERO-exception procedures.

## 5. Policy Compliance

5.1.1 **Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.2 **Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

5.1.3 **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6 Related Standards, Policies and Processes

None.

## 7 Definitions and Terms

None.

## 8 Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| **February 2022** | GP Hero Policy Team | New Policy |
| | | |