

Password Protection Policy

Last Update: *February 2022*

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to GP HERO systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords. 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

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any GP HERO facility, has access to the GP HERO network, or stores any non-public GP HERO information.

4. Policy

4.1.1 Password Creation

4.1.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.1.3 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all

other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

4.1.2 Password Change

4.1.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

4.1.2.2 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.1.3 Password Protection

4.1.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential GP HERO information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.1.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.1.3.3 Passwords may be stored only in "password managers" authorized by the organization.

4.1.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.1.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.1.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.1.5 Applications must support authentication of individual users, not groups.

4.1.6 Applications must not store passwords in clear text or in any easily reversible form.

4.1.7 Applications must not transmit passwords in clear text over the network.

4.1.8 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.1.9 Multi-Factor Authentication

4.1.9.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

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 |
| | | |