Internet Usage Policy

Last Update: *February 2022*

1. Overview

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

- Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.
- All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.
- Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by GP HERO Staff members and affiliates. The 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 Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to

comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.1. Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.
- File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
- Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorized access to/from the Internet and will not be allowed.

3.2. Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

3.3. Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

3.4. Approval

Internet access is requested by the user or user's manager submitting an IT Access Request form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

3.5. Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

4. Policy

4.1.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.1.2 Computer workstations must be locked when workspace is unoccupied.

4.1.3 Computer workstations must be shut completely down at the end of the work day.

4.1.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.1.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.1.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.1.7 Laptops must be either locked with a locking cable or locked away in a drawer.

4.1.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.1.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

4.1.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.1.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

4.1.12 Lock away portable computing devices such as laptops and tablets.

4.1.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

4.1.14 All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

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