Information Technology (IT) Systems and Communications Policy

This document defines information related to the use of IT systems, GPA system access, and annual cyber security training. GPA's Operating Officer is responsible for enforcing this policy, and non-compliance with this policy may result in disciplinary action and suspension of access to GPA's IT systems.

General Use of GPA IT Systems

All employees must use GPA's IT and communication facilities sensibly, professionally, lawfully, and consistent with their duties.

All use of GPA IT systems must be in accordance with this policy and any other rules and procedures.

All information relating to clients and business operations is confidential and must be treated with utmost care.

Employees must be mindful of intellectual property rights. Downloading, uploading, posting, copying, possessing, processing, and distributing materials from the internet may be an infringement of copyright or other intellectual property rights.

Employees must be mindful when using email, GPA company blog, or internal message boards as a means of communication because all expressions of fact, intention, and opinion in an email may bind employees and/or GPA and can be produced in a court of law in the same way as other kinds of written statements.

All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. Employees must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context, such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion, or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be, construed as bullying or harassment by the recipient).

Employees are assigned individual user accounts on GPA's IT system. It is prohibited for employees to share their login information with other employees, contractors, or external persons.

Use of Electronic Mail - General

Except where specifically authorized by the other person, employees are not authorized to access any other person's inbox or other email folders nor send any email purporting to come from another person.

Employees must note that copying an email to others may breach the Data Protection Act if it reveals all of the recipients' email addresses to each recipient (e.g., in the case of marketing and mailing lists). It can also breach duties of confidentiality (e.g., in the case of internal emails to members of a staff benefit scheme). Accordingly, it may be appropriate to use the 'bcc' (blind carbon copy) field instead of the 'cc' (carbon copy) field when addressing an email to more than one recipient.

Use of Electronic Mail – Business Use

All business email should include the appropriate GPA business reference.

Employees sending important documents via email should always telephone to confirm that the email has been received and read.

Employees filing or deleting any emails or attachments are required to file a hard copy or electronic backup. The same applies to all internal email transmissions concerning business matters.

In light of the security risks inherent in some web-based email accounts, personal web-based accounts should not be used for business.

Employees are responsible for ensuring price sensitive or highly confidential documents are not send to a customer's personal web-based email account.

Use of Electronic Mail – Personal Use

Employees are permitted to use their GPA email accounts for personal use on the condition that all of the procedures and rules set out in this policy are complied with.

Employees need to be aware that they can expect very little privacy since GPA may need to monitor communications for the reasons given in GPA's policies on IT system security.

Under no circumstances, may employees use GPA facilities in connection with the operation or management of any business other than that of GPA or a client of GPA, unless express permission has been obtained from the Board of Directors.

All email contained in an employee's inbox and sent items box are deemed to be business communications for the purposes of monitoring.

Employees must ensure that personal email use:

- Does not interfere with the performance of duties.
- Does not take priority over work responsibilities.
- Is minimal and limited to taking place substantially outside of normal working hours (i.e., during any breaks or before or after normal hours of work).
- Does not cause unwarranted expense or liability to be incurred by GPA.
- Does not have a negative impact on GPA in any way.
- Is lawful and complies with this policy.

Employees must acknowledge that personal email may be copied (perhaps many times) onto GPA's backup systems and in that form will be retained indefinitely.

By making personal use of GPA's facilities for sending and receiving email, employees signify their agreement to abide by the conditions imposed for their use and signify their consent to GPA monitoring personal email in accordance with any applicable GPA's policies on IT system security.

Use of Internet/Intranet

Any activity an employee engages in via the internet may affect GPA.

GPA recognizes the need for individuals to have to carry out some personal tasks during working hours, e.g., for internet banking or online shopping, and this is permitted subject to the same rules as are set out in the "Use of Electronic Mail – Personal Use" of this policy. If these activities require additional software to be installed onto GPA equipment, an employee should contact their supervisor who will consider the request in line with GPA policy.

Employees are strongly discouraged from providing their GPA email address when using public websites for non-business purposes, such as online shopping. This must be kept to a minimum and done only where necessary.

Use of GPA IT Equipment for In Office and Remote Employees

Employees working part-time or full-time from home are responsible for ensuring proper IT equipment is available to complete all assigned tasks.

GPA provides employees designated as remote with standard computer equipment, such as monitors, keyboards, cameras, or desktop machines. Any employee taking such equipment is required to obtain approval from their supervisor and the Operating Officer. In addition, employees must sign GPA's equipment distribution form and ensure the correct equipment is recorded.

Employees taking desktops or other equipment with firmware, operating systems, or similar software are required to ensure the equipment software is up to date and in line with GPA's Software Update, Patch, and Configuration Policy.

Employees are issued with a VPN certificate upon request. Employees may not distribute their certificate under any circumstances.

Employees are responsible to ensure any equipment, including GPA-issued and personal equipment, which is connected to GPA's VPN is in compliance with GPA's Cyber Security Incidence Reporting Procedure and Software Update, Patch, and Configuration Policy.

Employees are encouraged to avoid using removable media such as USB storage drives, memory cards, floppy disks, or similar equipment. GPA provides secure online storage for these purposes. Should it be unavoidable, employees must use GPA-issued equipment and any removable media that comes into contact with a non-GPA system must be scanned and approved by designated personnel before being reconnected to GPA systems.

Employees who are leaving GPA are required to return any GPA issued equipment on their last day of employment. GPA will treat returned equipment as external and not connect it to GPA systems until designated personnel have performed scans and approved the equipment.

GPA-issued equipment is not to be taken out of the United States without prior approval from the employee's supervisor and the Operating Officer or Board of Directors. Any employee taking GPA equipment out of the United States is required to ensure no one except the employee accesses that equipment.

Any employee who loses GPA equipment, whether by theft, destruction, or other means, or believes their account is compromised, is required to inform GPA as soon as feasible. Lost equipment will be considered external and will be removed from access to any GPA system or data as soon as technically feasible. GPA keeps a detailed record of any equipment lost and regularly scans its system to identify any vulnerability due to lost equipment or known compromised accounts.

Access to GPA IT Systems

All employees are issued IT accounts to access GPA's systems. Employees are prohibited from sharing their account information with others, including other employees.

Employees who need access to restricted IT support systems, including, but not limited to Active Directory, DHCP servers, and web servers, are issued Domain Administrator (DA) accounts in addition to their standard accounts. Issue of a DA account requires approval from the Operating Officer.

Employees are required to use their standard IT account whenever possible. Should a task require the use of the DA account, employees should note that the use of a DA account is logged and reviewed regularly.

Employees who need additional software for the performance of job-related tasks are required to ensure any additional software installed on their equipment meets GPA's Software Update, Patch, and Configuration Policy.

Physical access to GPA's server room is restricted to authorized personnel for job related tasks only. All requests for access must be approved by the employee's supervisor and the Operating Officer.

GPA provides the physical access request form to track access requests to the server room. Requests for physical server room access expire after 365 days unless otherwise recorded in the form.

In rare circumstances, authorized employees may escort another employee or contractor into the server room. Employees are responsible to ensure unauthorized, escorted personal only access the specific systems necessary to perform their assigned task.

Wireless Access to GPA IT Systems

GPA maintains a wireless network within its offices. This network is secured and encrypted at all times. Any access to the wireless network is subject to the same policies as access to the wired GPA network.

Mobile Devices and Access to GPA Systems

Pocket computers, mobile telephones, and similar hand-held devices are easily lost or stolen. Employees must password-protect access to any such devices on which is stored any personal data of which GPA is a data controller or any information related to our business, our clients, or their business.

Employees must report the theft of any mobile devices with access to GPA systems as soon as possible to their supervisor and the Operating Officer.

Public Communications

Employees may occasionally make public statements related to GPA.

Any statements that are made representing GPA are required to be approved by the Operating Officer or the Board of Directors.

Employees are permitted to express their own views and opinions as long as they clearly state these statements DO NOT represent GPA or its Board of Directors unless otherwise approved by the Operating Officer or a member of the Board of Directors.

GPA Operating Officer: Christoph Lackner (Signed Electronically)

