SAGH Information Technology ("IT") Policy

1. General

a) The Company IT policy does not address every possible situation: rather, it establishes a framework of actions and activities that relate to the use of the Company IT infrastructure. The fact that a particular activity or situation may not have been expressly prohibited, does not imply that such an activity is authorized. If you have any doubt, you must contact the IT Department for clarification before acting.

b) The Company IT infrastructure provides shared applications and resources used by the whole Company. You are therefore expected to appreciate that your actions in contravention of the IT policy will have a detrimental effect on you, the company and your co-employees.

c) You are required to safeguard the Company's information process data base and client particulars and you are required to take all reasonable steps to ensure that such information is not divulged to any person outside of the Company, or to any other employee of the Company who does not require such information in the performance of their regular duties.

d) The Company's IT policy will be reviewed periodically and may be amended due to the constant technological evolution of the Company's IT infrastructure, IT infringements and legislation generally.

2. Equipment

a) All IT facilities, equipment, photocopy, printing and fax facilities, information (data), software and/or any associated device/s residing on or used in conjunction with the Company IT infrastructure, shall remain the sole & absolute property of the Company.

b) The "workstation" you may be provided with as part of your work-related equipment and the type/specifications thereof (e.g. laptop, desktop etc.) will be determined on a per user basis, which will be at the Company's sole and absolute discretion.

c) You are therefore expected to utilize any IT hardware, software systems and information provided to you by the Company strictly for work related purposes and for the benefit of the Company only.

d) The IT department is responsible for the procurement, installation and maintenance of all computer hardware residing on the company network infrastructure. Accordingly, neither you nor any third party, is permitted to connect any hardware and/or peripheral device not supplied by the IT Department, to the Company's network and/or related equipment.

e) You are prohibited from disconnecting or dismantling, or allowing a 3rd party to disconnect or dismantle, any hardware and/or peripheral device from the Company's network.

f) If you wish to connect or disconnect any hardware device/s, you are required to obtain written permission/consent from the IT Department.

Software:

g) You are prohibited from loading, unloading and/or configuring any software on any Company IT system, or allowing a 3rd party to do so, without the approval of the IT Department. This restriction applies to commercial software, shareware and freeware.

h) You are expressly prohibited from using Company facilities to make illegal copies of licensed or copyrighted software. Copyrighted software may only be used in accordance with its license or purchase agreement

i) You are prohibited from using any type of destructive software whatsoever that is designed, for example, to destroy data, provide unauthorized access to computer systems, facilitate fraud and/or disrupt system processes in any way. The use of viruses, worms, Trojan horses, and other invasive software is strictly forbidden.

j) The Company installs anti-virus software on all of its computer systems, and you are required to use it. You are prohibited from tampering with this software or from turning it off. All external storage devices inserted into the Company's computers must first be scanned for viruses or other forms of malicious software. If you receive warnings about viruses, please forward the information immediately to the IT department. Employees must immediately report any malfunction that might be related to a computer virus to the IT department.

k) If you wish to load, unload and/or configure any software you are required to obtain assistance from the IT Department.

3. Security and Access Control

a) Your password will allow you to access those portions of the IT system you are authorized to access. Access to certain network resources may require you to obtain the written permission/consent of the IT Department. You are not permitted to access or assist any other person to access IT resources you or they are not authorized to use.

b) You are expected to treat the contents of electronic files as private and confidential.

c) Any misuse of computing resources or potential "loopholes" in network security must be reported to the IT Department and you agree to cooperate fully in the investigation of abuses.

d) You will be supplied with one or more means of user identification which will grant you access to specified authorized services and/or facilities in conjunction with your own unique password/s. You may not divulge your user identification and/or password/s to any other party (except see v below). You will be held directly liable/responsible if a Company device and/or user identification and/or password/s is used for any unlawful purpose, including contraventions of the Company IT policy.

e) You are obliged to disclose your user identification and/or password/s to any authorized IT Department personnel immediately upon request.

f) Network accounts cannot be shared, transferred or used by other employees. You may not use network resources to misrepresent yourself as another employee ("spoofing").

g) You are not to interfere with the access rights of other employees.

h) You must "log off" from workstations when you leave at the end of each working day and you must "lock" your workstation at all times when leaving your workstation unattended.

i) You may not engage in any activity that is intended to circumvent system security controls. This includes, but is not limited to, hacking which is defined as attempting (either successfully or unsuccessfully) to break into/or gain unauthorized access to a computer system or network; cracking of user accounts and/or passwords; deletion of production data; the making of unauthorized changes to production data; attempting to discover unprotected files; attempting to decode encrypted files and penetrate computer systems for unauthorized use.

j) You may not copy directories unless prior written permission/consent has been granted by the IT Department.

k) After the termination of your employment with the Company for any reason whatsoever, you have no right to access or use anything on the Company IT network.

4. Access to External Computer Systems

a) You may not use the Company computer systems to access or attempt to access networks and/or computer systems other than those authorized for your use. This includes, but is not limited to, the internet, extranets, intranets, e-mail, files, folders and directories.

b) When external networks and/or computer systems are authorized, they may only be used for Company-related business. In addition, the downloading and/or storing and/or printing and/or e-mailing of undesirable/hateful/obscene/pornographic material is not permitted. You may not download and/or store programs and/or software that are not approved by the IT Department.

5. Email and Internet Usage

In addition to what is set out above, the following applies:

a) All e-mail correspondence must be sent and received through the Company's system, which contains the information and disclaimers that the Company requires on all e-mails and telefaxes.

b) Large e-mail messages must be transmitted after normal working hours, unless critical in nature. If you experience difficulties in sending a large e-mail document, you should consider using compression utilities such as WinZip, or contact the IT Department for assistance in the use of alternative methods.

c) The Company shall not be held liable in the event that you store or use confidential information such as passwords and credit card information on the Company computer system which results in your suffering loss for any reason whatsoever.

d) The Company reserves the right to block any site deemed to be inappropriate.

e) Internet use, and indeed the use of all Company resources, is restricted to work-related issues and may not be used in the commission of any unlawful activity whatsoever, whether of a civil or criminal nature, or in any way calculated to overburden the resources of the Company.

6. Information Storage and Usage

a) You are encouraged to save work regularly. You are prohibited from storing personal information on the network and/or any IT device/s belonging to the Company.

b) You may not remove or copy any resource owned or licensed by the Company.

7. Monitoring

a) Please note that every database contained on or connected with the Company's computer system (including the information on any PC or laptop used by you to perform duties for the Company) is the Company's property. Furthermore, the company has the express right to monitor the use of all IT and telephone systems and related resources, and you may not, for any reason whatsoever, or in any manner whatsoever, refuse access. Accordingly, by your signature hereunder you acknowledge and accept that no privacy whatsoever attaches to any such information. Furthermore, you hereby consent to the Company accessing, for any reason deemed necessary in its sole and absolute discretion, any information contained in a database referred to in herein.

b) You are therefore warned that the Company has unlimited access to everything you do in connection with the IT system and you cannot refuse the Company such access for any reason whatsoever, especially if you are engaged in behaviour that is unlawful, contrary to your employment agreement with the Company, or in manner effects the Company's interests. Additionally, you cannot object if private or embarrassing material comes to the knowledge of the Company, as such material should not in any event be dealt with at work.

c) The Company reserves the right to test and monitor security and review any files or information resident on any systems allegedly related to unacceptable use.

d) The Company shall have the right, at all times (including in your absence) to access any employee's files, folders and/or messages, in its sole and absolute discretion.