



SITE SERVICES
HOLDINGS

COMPUTER AND NETWORK USAGE POLICY

Rev Number	Issue Date	Prepared By	Signature	Client Approval	Date	Signature
Rev 1	10/05/2017	P. Torre				



CONTENTS

1. INTRODUCTION	3
2. PURPOSE	3
3. SCOPE	3
4. SERVICES ACCESS	3
5. NETWORK LOG ON	3
6. RESPONSIBILITIES	4
7. USAGE	5
8. EMAILS	6
9. MONITORING	7
10. CONSEQUENCES OF VIOLATIONS.....	7



1. INTRODUCTION

Site Services Holdings (SSH) computer and communications network allows access to resources and services through internet, intranet, electronic mail and telecommunication services (“Service”) connectivity. This document formally defines our official policy regarding Service usage and all Service users are expected to be familiar with and to comply with this policy.

2. PURPOSE

SSH is committed to preventing the occurrence of inappropriate, unethical, or unlawful behaviour by any of the users of its computing systems and telecommunications networks. These responsibilities are not only mandated by SSH business interests but by legal and ethical obligations concerning the welfare and privacy of its staff and business partners. This Network Usage Policy and its strict enforcement is an important and necessary part of the overall usage strategy.

3. SCOPE

Access to the Service is provided to support business activities only. The Network 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 Service through the computing or networking resources. The Company’s Service 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 judgement while using the Service

4. SERVICES ACCESS

1. Request and Approval Procedures
Internet access will be provided to users to support business activities and only as needed to perform their jobs.
2. Removal of Privileges
Service access will be discontinued upon termination of an employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy.

5. NETWORK LOG ON

Every SSH employee authorised to use the SSH Service is provided with a unique personal login profile including a user name and password. The password is a critical security feature of SSH Service and



must be kept strictly confidential at all times. Any employee inappropriately sharing a password or failing to properly secure and maintain the confidentiality of the password may be disciplined.

6. RESPONSIBILITIES

Additionally, you must not:

- Intentionally violate any applicable law;
- Post, transmit, link to, disseminate or otherwise distribute any unlawful material (such as child pornography or legally obscene material);
- Send, display, access, make available, publish, distribute, or otherwise be involved in material that is obscene, pornographic, defamatory, offensive or abusive or is or would be regarded by SSH or another person, acting reasonably in all the circumstances, to be, offensive or abusive; or store any such material on any SSH Service; or allow such material to remain present on the Service when you become aware or are made aware of it;
- Use the Service to access file sharing peer to peer sites, or other sites for the purpose of downloading personal music, video or software;
- Engage in fraudulent activities including forgery, impersonation, or forging another person's signature;
- Engage in activities which disseminate or incites discrimination, hate, violence, propaganda, contrary to law; or otherwise discriminates towards one person or group, for example, because of their race, religion, gender or nationality;
- Operate pyramid or other illegal soliciting or fund raising schemes or be involved in any gambling or gaming activities;
- Disseminate material which violates the copyright, moral rights or other intellectual property rights of others;
- Defame, abuse, stalk, harass, or threaten others;
- Otherwise violate the contractual, property or civil rights of others, including rights relating to privacy and publicity.
- Interfere with the proper operation of the Service or any part of SSH operations or a third party network or system.
- Use the Service to send out unsolicited e-mail, whether of a commercial nature or not, which degrades the performance of the network;
- Send e-mail messages to another individual or another system who has explicitly asked you to stop;
- Distribute chain letters, pyramid schemes, "Ponzi" schemes, or multi-level marketing scams;
- Improperly restrict, inhibit or degrade others' use of the Service;
- Use the Service to breach the security of another user, or to attempt to gain access to another person's computer, software or data, without the knowledge and consent of that person or to attempt to circumvent the user authentication or security of any host, network or account,



including accessing data not intended for your access, unauthorized logging into or making use of a server or account or probing the security of other networks

- Use the Service to interfere with (or encourage others to interfere with) computer networking or telecommunication services to any user, host or network, including denial of service attacks, flooding of a network, overloading a service, or attempting to crash a host;
- Distribute (or encourage other to distribute) spamware, mass e-mailing programs or technologies designed to overburden internet operations;
- Seize or abuse operator privileges
- Use or distribute tools designed for compromising security, such as packet sniffers, ping bombers, cracking tools, password guessing programs or network probing tools;
- Transmit or disseminate any information or software which contains a virus, cancel bot, Trojan horse, worm or other harmful or disruptive component; or
- Breach current bandwidth or data storage restrictions to the point where such breach degrades network performance
- Improperly restrict, disrupt or degrade SSH ability to maintain the network and deliver the Service or monitor the internet Service.
- Otherwise overburden the network or affect the ability to provide services.
- Remove computers/tablets from the work premise unless authorisation is obtained from the relevant Manager.

7. USAGE

1. Resource Usage

Access to the Service will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. User Service access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

2. Allowed Usage

Service usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgement in using the Internet. Acceptable use of the Service, including Internet, for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- Review of possible vendor websites for product information
- Reference regulatory or technical information.

3. Personal Usage

Using company computer resources to access the Service for personal purposes, without approval from the user's manager, may be considered cause for disciplinary action up to and including termination. All users of the Service should be aware that the company network



creates an audit log reflecting request for Service, both in-bound and out-bound addresses, and is periodically reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet “wallets” do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property. The Company discourages the use of non-Company provided equipment for business purposes. Employees should use Company provided hardware and software in the course of their business duties. SSH General Manager must approve all employee-owned personal computer equipment before it may be used in connection with the Company’s Resources. While attached to the Company computer or network, personal equipment may be subject to incidental access while the Company is maintaining Company-owned devices. For example, the Company has the same authority to access a non-Company owned hard drive attached to Company owned equipment as it has to access Company-owned equipment. SSH is not responsible for the repair, replacement or support of non-Company owned hardware or software.

4. Software License

The Company strongly supports strict adherence to software vendors’ license agreements. When at work, or when company computing or networking resources are employed copying of software in a manner not consistent with the vendor’s license is strictly forbidden. Similarly, reproduction of materials available over the Service must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of “fair use” is in keeping with international copyright laws. Software must be purchased and installed by IT.

5. Maintaining Corporate Image

When using company resources to access and use the Internet, users must realise they represent the company and users must not place company material (examples: internal memos, press releases, product or usage information, documentation etc) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee’s manager and will be placed by an authorised individual.

6. Company Data/File Access All SSH personnel must ensure that company data/files are:

- Stored in the appropriate directory
- Not to be copied to personal/home pc/laptop or USB
- Every endeavour will be made to protect the integrity/security of company data/files

8. EMAILS

1. E-mail is an accepted official channel for communication.



2. It is the employee's responsibility to check and process their e-mail in-box as they would their hard copy in- tray.
3. E-mail messages may form valid evidence, just as hard copy documents do. Accordingly, e-mail messages are to be sent and treated the same way as we currently treat hard copy documents e.g.
 - Validation (if required) by the appropriate Department Head / Manager.
 - Construct e-mail messages as you would memos or letters.
 - Retention periods for e-mail messages correspond to those specified for hardcopy documents.
4. E-mail shall only be used for Company and not personal business. It is each employee's responsibility to use the facility provided for the purpose of carrying out work. The e-mail network, including messages and their contents, belongs to the Company and therefore the Company has the right to access e-mail messages if necessary.
5. Employees should be aware that any e-mail messages that they send distributing any third party information are subject to normal Copyright Law.
6. MSN Messenger and similar services are not an accepted channel for communication and are not to be used for business nor personal communications.

9. MONITORING

Users should consider their Service activities as periodically monitored and limit their activities accordingly. SSH reserves the right to examine e-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice, but is not obliged to do so. This examination ensures compliance with internal policies and assists with the management of company information systems. SSH may investigate any misuse or suspected misuse of the Service and may involve the police or other law enforcement agencies in doing so. SSH may recover the cost of such investigation if it is established that you have misused the Service. If your use of the Service causes any loss or damage to third parties, you must compensate those third parties for such loss or damage. SSH reserves the right to withdraw your access to the SSH Service, at any time without notice, if SSH believes you may have engaged in any prohibited use of Service.

10. CONSEQUENCES OF VIOLATIONS

Violations of the Computer and Network Usage Policy will be documented and can lead to revocation of Service privileges and/or disciplinary action up to and including termination. Additionally, SSH may at its discretion seek legal remedies for damages incurred as a result of any violation. SSH also reserves the right to report illegal activities to the proper governmental authorities and to assist them in any



prosecution. Before access to the Service via company network is approved, the potential internet user is required to read this Network Usage Policy.