June 2011

Electronic Communication IT Policy

FOSITGOV-002

Revision 3

FOS IT Policy

IT Policy

Issued – 28 Aug 2010

ELECTRONIC COMMUNICATION POLICY

For: FIRSTONSITE Users

Copies: FILE

i) Document Control:

Version	Revision Date	Revision Description	Author
Draft 1.0	June 12, 2008	Draft v 1	JL. Marin
Rev 1.0	Sept 11, 2008	Rev 1	JL. Marin
Rev 2.0	Sept 28, 2009	Rev 2	JL. Marin
Rev 3.0	August 10, 2011	Rev 3	N. Belcher

ii) Abstract:

This document is to be used as a Policy. This document details how security is enforced from an end to end process perspective. Policies governing the use of computer resources and e-mail are defined under the corporate Policy for Information Technology. Please refer to the Corporate IT User Policies and Standards for additional information.

iii) Disclaimer of liability for use of Internet:

.

The Company is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

1) Introduction:

FirstOnSite Restoration L.P. (FOS)(the "Company") provides internal electronic mail (ClaimTrak Message Posts.) and Internet electronic mail ("e-mail", "Outlook", "Exchange", "Spark Messenger", "Instant Messaging", "IM") as an efficient means of business communication. Certain employees may be provided with access to the Internet/Intranet/Extranet (the "Internet") to assist them in performing their job functions.

While the Company acknowledges that occasional personal use of e-mail/IM and the Internet may not be inappropriate in moderation, these tools are owned by the Company and were brought into the Company to improve customer service and increase productivity. This policy sets out acceptable standards for e-mail, instant messaging and Internet use. Personal use of e-mail, IM, or the Internet should in no way adversely affect work performance or productivity.

The Internet can be a valuable source of information and research. In addition, e-mail and IM can provide excellent means of communicating with other employees, our customers and clients, outside vendors, and other businesses. Use of the Internet, however, must be tempered with common sense and good judgment.

Non Compliance Consequences

If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible termination, and civil and criminal liability.

Violation of the provisions of this policy may result in disciplinary action being taken against the user, up to and including dismissal. Some activities (among others) that will result in discipline are pornography, gambling, harassment or any illegal activity.

Your use of the Internet is governed by this policy and the E-Mail Policy. Any violation requires the consultation of the Director of I.T. and the CHRO.

2) Company Property

All computer equipment and accessories, personal computers, laptops, servers, and handhelds (purchased by FOS), including without limitation to any and all communications, documents, data, intellectual property developed, information and messages accessed, created, stored, sent, received or viewed using such equipment are the exclusive property of the Company.

3) Representative of the Company

When surfing the Internet or sending e-mail or IM from the Company computers, users are reminded that they are representatives of the Company to the outside world. Simply connecting to a website causes the user's name and the Company Internet address to be recorded on that remote computer.

Views expressed in e-mail or IM by a user may be perceived as the views of the Company. Accordingly, users should identify themselves properly (i.e., they should ensure that a personal view is not interpreted as being that of the Company).

All use of e-mail, IM and the Internet should involve good judgment, common sense and careful discretion.

4) Style of Communication

Users should assume that their message may be seen by people other than the intended recipient and that a hard copy may be printed out for file records. Highly informal e-mail and IM messages may be embarrassing to the sender and to the Company; accordingly, e-mail and IM should be composed keeping this caution in mind.

5) Insecurity of E-Mail

Keep in mind that the Internet is a public and insecure medium and users have a responsibility toward ensuring that Company and client information is protected. Since the sender has not a guarantee of privacy and no control over whether an e-mail or IM message is copied, modified or forwarded to a wide audience without his/her knowledge or consent once the message has been sent, steps must be taken to protect sensitive material.

In order to maintain confidentiality, before sending sensitive documents to customers as enclosures via Internet e-mail, transmission of such documents must be pre-cleared with the customer receiving the material so that he/she understands potential risks. If desired, arrangements may be made for the documents to be encrypted so that they cannot be intercepted during transmission.

For assistance with sending encrypted confidential documents by e-mail or IM, contact the Information Technology Department.

All Internet e-mail messages must include a caution which reads as follows:

Although it has many advantages, e-mail and IM can be abused more readily than other forms of communication. Forgery (or attempted forgery) of e-mail or IM messages is prohibited. Attempts to read, copy, modify, or delete e-mail or IM messages of other users without their permission (other than authorized monitoring by the Company) is prohibited.

Users should also be mindful that e-mail or IM messages, even when deleted from their files, may remain in the memory of a computer or in the Company tape back-ups until they are overwritten. E-mail or IM messages may have to be produced in litigation and may be capable of being retrieved even if they have been deleted.

The computers and computer accounts given to employees are to assist them in performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the Company and may only be used for business purposes.

6) Inappropriate Material

Users are prohibited from accessing, posting, storing, downloading, transmitting and/or distributing information from inappropriate sites which might be illegal, threatening, abusive, libellous, defamatory, obscene, or viewed as offensive to others (e.g., pornography, racist literature and hate literature). Users are cautioned that accessing material which may be offensive to others may be in violation of the Company's sexual harassment policy.

Sending harassing, threatening or other objectionable messages via e-mail/IM is prohibited, as is sending unsolicited junk mail, for profit messages or chain letters.

7) Accessing the Internet.

To ensure security and to avoid the spread of viruses, employees accessing the Internet through a computer attached to FIRSTONSITE's network must do so through an approved Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless the computer you are using is not connected to the Company's network.

8) Virus detection.

Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files

attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses that may damage the Company's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. If you suspect that a virus has been introduced into the Company's network, notify the Help Desk immediately.

(Contact the Helpdesk for the installation of AV tools.)

9) Sending unsolicited e-mail or IM (spamming).

Without the express permission of their supervisors, employees may not send unsolicited e-mail or IM to persons with whom they do not have a prior relationship.

10) Use of Internal Distribution Lists.

Use of internal email distribution lists (re: DL-FOS-FirstOnSite Employees) is strictly reserved for upper management and should be used sparingly. Please do not use this DL's without first getting your supervisor's permission. Never copy a DL once received.

11) Monitoring of System

E-mail and IM sent within the Company is secure, although the Company does not consider e-mail or IM to be private communication by employees and reserves the right to monitor all Internet use and read all aspects of any e-mail or IM sent or stored within the system without further notice to the user. In addition, the Company has an Internet monitoring system in place which is able to track websites which users have visited.

The Company has the right, but not the duty, to monitor any and all of the aspects of its computer system, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail/IM sent and received by users.

12) Blocking of inappropriate content.

The Company may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Company networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to company blocking software.

13) Downloading Programs

Because of the prevalence of viruses on the Internet, downloading of any executable programs, except as expressly approved by the IT Department, is prohibited. When

approved by the IT Department, downloading of materials must be done on your specific PC's hard drive, and not to the Company's network servers, unless otherwise authorized/instructed by IT.

14) Games and entertainment software.

Employees may not use the company's Internet connection to download games or other entertainment software, including wallpaper and screen savers, or to play games over the Internet.

15) Purchases

Personal purchases are not to be made over the Company Internet connection and company purchases are only to be made in accordance with Purchasing Department policy.

16) Copyright

The normal laws of copyright apply to all materials on the Internet. Copying or distributing such materials without the prior consent of the owner of the copyright or license may constitute infringement. Users should treat the Internet the same way they would treat other sources of information.

17) Illegal copying.

Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy.

You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Chief Human Resources Officer.

18) Prohibited activities.

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, inappropriate, offensive (including offensive material concerning sex, race, color, national origin, religion, age, disability, or other characteristic protected by law), or violations of FIRSTONSITE's equal employment opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or stored in FIRSTONSITE's computers.

Employees encountering or receiving this kind of material should immediately report the incident to their supervisors or the Human Resources Department. FIRSTONSITE's equal employment opportunity policy and its policies against sexual or other harassment apply fully to the use of the Internet and any violation of those policies is grounds for discipline up to and including discharge. Such violations are also a breach of the Human Rights Code and violators will be subject to provincial law.

19) Accessing Remote Systems

Use of the Company computer systems in attempt to gain unauthorized access to other systems is prohibited.

20) Duty not to waste computer resources.

Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

Because audio, video and picture files require significant storage space, files of this or any other sort may not be downloaded unless they are business-related. This includes but is not limited to: Internet Radio Stations, Streaming Audio, Streaming Video, "YouTube", POD Casts, etc...

21) Reporting Offences

Breaches of this Policy should be reported to the Director of I.T., who in consulting with the CHRO will determine appropriate consequences.

22) Vacation Alert

It is recommended that employees use the "Out of Office" feature in e-mail to automatically advise others when they are away from the office for extended periods of time. Details on using this feature can be obtained by contacting the IT help desk.

Do not email your vacation alert, unless directed at your immediate coworkers or team members, never email your vacation alerts by way of internal Distribution Lists.

23) Changing Passwords

Employees are advised to change their system passwords periodically. On Policy all users are required to change their passwords every six months at a minimum.

24) Amendments and Revisions.

This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

Use of the Internet via FIRSTONSITE's computer system constitutes consent by the user to all of the terms and conditions of this policy.

25) Related procedures / documents

ITBOK (IT Body of Knowledge):

Our ITBOK and training documentation is available on our Intranet located at:

http://my.firstonsite.ca/training/ITBOK