COMFORT SYSTEMS USA
Design Mechanical, Inc.

Technology Use Policy

Section 1. Introduction

Comfort Systems USA, Inc. and its subsidiaries (collectively the "Company") use many communications and information technologies. These technologies, when properly used, support the Company's business activities and facilitate communication within the Company and with the Company's clients and vendors. These guidelines and policies are intended to minimize the likelihood of careless use of the Company's communications and information technologies by educating the Company's employees, and also by serving as the Company's written policies.

These guidelines address the appropriate use of electronic "Communications Tools" at the Company. These Tools include the following communication devices and information systems:

a) Company-supplied telephones (including landlines, cellular phones, and "smart" phones), pagers, voicemail facilities, portable communication devices, and portable digital assistants;
b) E-mail accounts;
c) Wireless communications devices;
d) Company-supplied fax machines, modems and servers;
e) Company-supplied computers (including laptops);
f) Company-supplied network tools (like browsers and Internet access facilities); and
g) Company-supplied and licensed software and applications.

Section 2. Use and Misuse of Communications Tools

2.1 Access. Access to Company Communications Tools is provided in conjunction with the Company's business and your job responsibilities. Your use of these Communications Tools is subject to this policy and to other Company policies and procedures. Communications Tools and all messages produced or carried by such Tools are Company property, subject to reasonable Company inspection.

2.2 Acceptable Use. In the course of your job, you may use these Communications Tools to communicate internally with Company co-workers or externally with customers, consultants, vendors, and other business acquaintances. The Company provides you with Communications Tools to facilitate business communications and to enhance your productivity. There may be occasion to use these Communications Tools for personal purposes. Personal use is permitted so long as it does not interfere with the performance of your job, consume significant resources, give rise to more than nominal additional costs, interfere with the activities of other employees, involve unacceptable content, or violate the Company's Social Media Best Practices. Under no circumstances shall such Communications Tools be used for personal financial gain, to solicit others for activities unrelated to the Company's business, or in connection with political campaigns or lobbying.

In addition to other restrictions and conditions discussed here, you may not use any Communications Tool:

- to carry any defamatory, discriminatory, or obscene material;
- in connection with any infringement of another person's intellectual property rights (e.g., copyrights);
- in a manner that violates the terms of any applicable telecommunications license or any laws governing data flow (e.g., laws dealing with data collection, protection, privacy, confidentiality, security, or encryption);

- in connection with any attempt to penetrate the computer or network security of any Company or other system, or to gain unauthorized access (or attempted access) to any other person's computer, e-mail, voicemail accounts, or equipment;
- in connection with the violation or attempted violation of any law;
- to send confidential information without the proper protections;
- to express personal opinion as Company opinion;
- to send chain letters or solicitations;
- to mislead the recipient of any message as to the actual identity of the sender; or
- for excessive personal use.

The Company understands that web "surfing" may be business-related and serve a legitimate business function, but the potential for abuse exists. There is no single, comprehensive directory of resources available for the Internet and users sometimes must "navigate" through much unneeded information to reach useful material. The Company encourages exploration of the Internet for legitimate business-related or professional activities, but you should avoid "browsing the web" on Company time, creating personal "Home Pages," or otherwise using Company facilities to access Internet sites for reasons unrelated to the Company's business and your job responsibilities.

An employee who is classified as non-exempt for purposes of the Fair Labor Standards Act may not use Company Communications Tools to perform his or her job duties (including checking work e-mail or voicemail) other than during his or her normal work hours and at his or her normal place of work without prior authorization from the employee's immediate supervisor.

An employee who shares or distributes large data files in the course of performing his or her job duties for the Company may be given access to the Company's File Transfer Protocol ("FTP"). Any employee who uses the FTP must comply with the Company's FTP Procedures guidance, which may be updated from time to time and is available on the Company's intranet, at http://www.fixintranet.com.

2.3 Unacceptable Content. Although the Company does not regularly monitor voicemail or electronic messages, please be aware that even personal e-mail and voicemail messages may be viewed publicly or by Company management without further notice. Under no circumstances may any communication originating at the Company or from Company Communications Tools be in violation of the letter or the spirit of any of the Company's policies.

Examples of unacceptable content include:

- sexually explicit messages, images, cartoons or jokes;
- unwelcome propositions, requests for dates or love letters;
- profanity, obscenity, slander or libel;
- ethnic, religious or racial slurs;
- or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

No chain letters or solicitations are permitted. Employees who receive chain letters or other unacceptable content should delete the messages or files immediately and contact the IT Department if messages are received repeatedly from the same source. All employees should be aware that the standard for sexual harassment is whether the recipient could reasonably consider the message to be offensive – the sender's intentions are usually irrelevant. In addition to prohibitions on sending or uploading offensive materials, Company Communications Tools (e-mail, browsers, etc.) also shall not be used to access or download obscene materials or other "content" that may be illegal under local law.

From time to time, the Company prevents access on the Company's network to some Internet sites that it determines pose a particularly strong risk of facilitating or encouraging violations of this policy. However, in the interest of maintaining a flexible and comfortable workplace, the Company allows access to most Internet sites through the Company's network and filters designed to prevent access to inappropriate sites are not fool-proof. Employees are ultimately responsible for ensuring that they comply with this policy.

Additional guidance for the use of social media for business and personal purposes is provided in the Company's Social Media Best Practices, which may be updated from time to time and is available on the Company's intranet at http://www.fixintranet.com.

***2.4 Electronic Forgery*.** Electronic forgery is defined as misrepresenting your identity in any way while using electronic communications systems (e.g., by using another's e-mail account without permission, by so-called IP spoofing, or by modifying another's messages without permission). For example, messages written by others should be forwarded "as-is" and with no changes, except to the extent that you clearly indicate where you have edited the original message (for example, by using brackets [ ] or by using other characters to flag edited text). Electronic forgery is not allowed for any purposes.

2.5 Intellectual Property. The Internet offers a universe of information, useful in conducting and furthering business operations. You must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video, and audio material, software, information and inventions. Do not copy, use, or transfer others' materials without appropriate authorization. Be aware that downloaded software and other copyrighted material may be subject to licensing obligations or restrictions. Even when software is labeled "freeware" or "shareware" there may be retained licensing restrictions that prohibit or limit the usage or commercialization of such items. If you have any questions in this regard, contact your supervisor, the Office of the General Counsel, or the Chief Information Officer/IT Director for guidance.

2.6 "Hands-Free" Use of Communications Tools. If you are using the Company's Communications Tools while operating a motor vehicle, please use a "hands-free" option. If no "hands-free" option is available to you, please do not operate a motor vehicle while using the Company's Communications Tools.

***2.7 Unauthorized Duplication and/or Distribution of Licensed Software*.** The Company requires strict adherence to the software vendors' license agreements. No employee is permitted to use the Company's Communications Tools to copy, download, upload, and/or transmit any documents, software, images, or other information protected by copyright or other proprietary rights without obtaining proper consents and licenses.

2.8 Consequences of Misuse. Misuse of any Company Communications Tool or violations of this Technology Use Policy may result in disciplinary action up to and including termination from the Company.

Section 3. Limits of Privacy

3.1 Retention and Security of Messages. E-mail and voicemail messages, and computer-stored items all are Company property and business records, and may have operational effect identical to that of traditional, hardcopy documents. Accordingly, all e-mail messages should be treated as though others may view them at a later date. Remember that no electronic communications facility is completely secure. This means that information stored on or carried over Company Communications Tools may be the subject of accidental or intentional interception, misdelivery, attack, or authorized Company review. When stored on computers, e-mail messages and other files typically are subject to routine back-up procedures. This means that in accordance with document retention procedures, copies of these files may be retained.

3.2 A Limited Expectation of Privacy. The Company respects the personal privacy of its employees. However, because Communications Tools are provided for the Company's business purposes, employee rights of

privacy in this context are extremely limited. Employees and others should have no expectation that any information transmitted over or stored on Company Communications Tools is or will remain private. These Communications Tools are owned and/or controlled by the Company and are accessible at all times by the Company for maintenance, upgrades, or any other business or legal purposes. Employees who use Company Communications Tools should be aware that the Company's Communications Tools create audit logs detailing every request for access in either direction by each user of the Communications Tools. Also, in the course of their duties, system operators and managers may monitor employee use of the Company's Communications Tools or review the contents of stored or transmitted data.

The Company permits limited personal use of all these Communications Tools on the express understanding that it reserves the right (for its business purposes or as may be required by law) to review employee use of, and to inspect all material created by or stored on, these Communications Tools. Use of these Communications Tools constitutes each employee's permission for the Company to monitor communications and to access files that are made on or with these Communications Tools.

Section 4. Specific Guidelines for Internet Usage

4.1 Internet and Your Data. The Internet is an unsecured network. All data sent across the Internet is sent in clear text. This means any e-mail messages, files transferred, etc., are sent in such a manner that anyone can read the information. Keeping this in mind, appropriate security measures should be used when transferring any company sensitive or confidential information.

4.2 Internet File Transfers. One threat the Company has to deal with from the Internet is the potential of viruses being brought into the Company's internal networks from Internet sources. As such, no employees of the Company is allowed to download any programs for downloading music and/or videos onto any Company computer system, including any software designed to access any peer-to-peer file sharing networks, unless approved in advance by the Chief Information Officer/IT Director. Additionally, all executable files downloaded from the Internet must be virus checked before being run on any Company computer system.

4.3 Internet Logs. The Company's security requirements authorize the Network Administrator to maintain logs of Internet activities. At any time, Internet transactions may be logged with the user's name, time of day, and what action has taken place. The Company may review these logs periodically.

Section 5. Reporting Security Problems

5.1 System Security. All system users have a duty to report all information security violations and problems to the Network Administrator or Chief Information Officer/IT Director of the Company on a timely basis so that prompt remedial action may be taken.

5.2 Immediate Reporting of Computer Viruses. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, all users have a duty to promptly report any computer viruses, even if the user's negligence was a contributing factor to introducing the virus to the Company's network. If a report of a known computer virus infection is not promptly made, and if an investigation reveals that certain system users were aware of the infection, these system users will be subject to disciplinary action up to and including termination of employment.

Section 6. Security Policy Compliance

6.1 Employees who lose or damage any Company Communications Tools in violation of this policy may, at the Company's sole discretion, be required to reimburse the Company for the full extent of the damage or lost equipment.

6.2 Frequently, Company Communications Tools will be configured to require that a password be entered at start-up, sign-in, and at each reactivation from sleep, hibernation, or similar "rest" mode. Employees may not disable this feature or otherwise program a Company Communications Tool so that a password is not required prior to each use. Any employee who receives a Company Communications Tool that is not password protected should enable the password feature and may contact the Company's IT department for assistance. This requirement does not apply to any Company Communications Tools that cannot be password protected, such as pagers, simple cell phones (i.e., not a "smart" phone), and landline telephones.

6.3 Any employee who uses a person communications tool to access or store a Company e-mail account, Company files, or other information acquired in the course of performing the employee's job du ties for the Company must ensure that the communications tool is password protected.

6.4 The Company has adopted a policy requiring that encryption software, of a kind approved by Chief Information Officer/IT Director, be installed on new notebooks, tablets, or other portable computers that house or are likely to house sensitive, confidential, or proprietary information. Employees may not disable or otherwise alter this software after its installation.

Section 7. Questions or Changes to Policies

Questions about this policy may be directed as appropriate to your supervisor, the Office of the General Counsel, or the IT Department. The Company intends generally to observe these policies but also reserves the right to change them at any time without prior notice. The Company will make reasonable efforts to provide notice of such changes by postings to the Company's intranet at http://www.fixintranet.com.

Last Revised August 2011