EXCELLENT FORTUNE DEVELOPMENT GROUP

Acceptable Use Policy

1. Overview

1.1 Internet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, storage and web browsing are the properties of the company. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

1.2 Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment in the company. These rules are in place to protect the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

3.1 This policy applies to the use of information, electronic and computing devices, and network resources to conduct the company's business, whether owned or leased by the company, the employee, or a third party. All employees, contractors, consultants and all other workers in the company and its subsidiaries, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the company's policies and standards, and local laws and regulation.

3.2 This policy applies to employees, contractors, consultants and all other workers in the company and its subsidiaries, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the company.

4. Policy

4.1 General Use and Ownership

4.1.1 The company's proprietary information stored on electronic and computing devices whether owned or leased by the company, the employee or a third party, remains the sole property of EFD Group. You must ensure through legal or technical means that proprietary information is protected.

4.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.3 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of the company's proprietary information.

4.1.4 You may access, use or share the company's proprietary information only to the extent authorized and necessary to fulfill your assigned job duties.

4.1.5 For security and network maintenance purposes, authorized individuals within the company may monitor the equipment, systems and network traffic.

4.1.6 The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3 Postings by employees from a company's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties.

4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the company authorized to engage in any activity that is illegal under local or international law while utilizing any company-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.

c. Accessing data, a server or an account for any purpose other than conducting the company’s business, even if you have authorized access, is prohibited.

d. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

e. Making fraudulent offers of products, items, or services originating from any of the company’s account.

f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

g. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

h. Circumventing user authentication or security of any host, network or account.

i. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

j. Introducing honeypots, honeynets, or similar technology on the company’s network.

k. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

l. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.

m. Providing information about, or lists of, the company’s employees to parties outside the company.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

c. Unauthorized use, or forging, of email header information.

d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f. Use of unsolicited email originating from within company's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by the company or connected via the company's network.

g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

a. Blogging and posting in social media by employees, whether using the company's property and systems or personal computer systems, is subject to the terms and restrictions set forth in this Policy.

b. The company's Confidential Information policy also applies to blogging and posting in social media. As such, Employees are prohibited from revealing any of the company's confidential or proprietary information, trade secrets or any other material covered by the company's Confidential Information policy.

c. Employees shall not engage in any blogging or posting in social media that may harm or tarnish the image, reputation and/or goodwill of the company and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments in any blogging or posting in social media.

d. Employees may also not attribute personal statements, opinions or beliefs to the company when engaged in any blogging or posting in social media. If an employee is expressing his or her beliefs and/or opinions in blogs or social media, the employee may not, expressly or

implicitly, represent themselves as an employee or representative of the company. Employees assume any and all risk associated with blogging or posting in social media.

e. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the company's trademarks, logos and any other the company's intellectual property may also not be used in connection with any blogging activity or posting in social media.

5. Policy Compliance

5.1 Compliance Measurement

The company will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the policy owner in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.