Improving of corporate security policy

Dear Richman Investments Senior Management, It has come to my attention that your corporate security policy for the firm is out of date and that it needs to be updated. In my time here as an intern I have reviewed the security policy and revised it to keep up with all of the technological updates going on in the internet world today. I was assigned this project and being that we have 5000 employees operating in different locations and different parts of the country; I have noticed that some of the other branches do not follow the firms' policies as they should.

Some branches operate on their own policies. I have drafted up a new and improved corporate security policy that covers emails, mobile devices, computer usage, email retention policies, passwords, etc. I hope this will help streamline our security policy across the board so that everyone is on the same page and so there is no misinterpretation of the firm employee or otherwise. RICHMAN INVESTMENTS CORPORATE SECURITY POLICY Use of Phone and Mail Systems Personal use of the telephone for long-distance and toll calls is not permitted.

Employees should Practice discretion when making local personal calls and may be required to reimburse The Firm for any charges resulting from their personal use of the telephone. The mail system is reserved for business purposes only. Employees should refrain from sending or receiving personal mail at the workplace. To ensure effective telephone communications, employees should always use the approved greeting and speak in a courteous and professional manner. Please confirm information received from the caller, and hang up only after the caller has done so.

Computer and E-mail Usage Computers and other media of electronic communications (" Media") are the property of the Firm which has a legitimate business interest in the proper utilization of its property. Therefore, any use of the Firm's property, and any electronic communications sent or received, may be monitored by persons authorized by the Firm. Employees who use such Media for private, non-work related purposes do so at their own risk. The Firm encourages such Media to be used for business purposes and forbids the waste or monopolization of such resources.

Electronic communications, including computer files, voicemail and electronic mail (" e-mail"), are not anonymous: sender and receiver can be determined, and the content of any message may be viewed by others within the Firm. A password is not intended to ensure the privacy of electronic communications. Instead, it serves to provide a minimum level of security to the Firm's Media by restricting access to those who bear valid passwords. Preventing a person from outside of the Firm from gaining access to the Firm's Media is not the same as affording privacy to the communications of Media users.

The Firm strives to maintain a workplace which is free of harassment and sensitive to the diversity of its employees. Therefore, the Firm prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial

comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

In addition, e-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. E-MAIL IS NOT A PRIVATECOMMUNICATIONWITHIN THE FIRM. NEVER USE E-MAIL TO SEND PERSONAL INFORMATION OR DISCUSS PRIVATE MATTERS ABOUT ANYONE, INCLUDING YOURSELF, UNLESS DISCLOSURE OF THAT INFORMATIONWITHIN THE FIRM IS ACCEPTABLE TO YOU. THIS PROHIBITION ALSO APPLIES TO VOICEMAIL AND COMPUTER FILES. ANY DEFAMATORY, INSULTING OR DEROGATORY REMARK ABOUT ANY PERSON OR GROUP OF PERSONS IS PROHIBITED.

Email Retention Policy Because the volume of e-mails sent and received continues to rise, the size of attachments Continues to grow, and pictures and images consume significant amounts of storage space, the Firm has Adopted an Email Retention Policy that addresses retaining, deleting and saving e-mail in an effort to Advance the Firm'stechnologyobjectives and ensure that a reliable network exists for rapid message exchange and communication. The Email Retention Policy allows a faster, more responsive e-mail system and ensures that, in the event of a disaster (i. . hardwarefailure, natural disaster events, etc.), our messaging services can be quickly restored to operation. This policy also encourages organization of e-mail through the use of email folders. The policy is designed to automatically delete information from only the Inbox, Sent Items and Deleted Items as they age. The Table below illustrates the policy and aging

and flow of email items from those folders. Software Policy The Firm will not tolerate any employee making unauthorized copies of software.

The Unauthorized duplication of software violates software licensing agreements and federal copyright laws. Such conduct is not only against the Firm's policy, it is a federal criminal offense. No employee shall install any software on any computer at the offices of the Firm unless the installation is approved in writing in advance of the installation. Social MediaPolicy Although this is not a complete or exhaustive list, employees should consider the following guidelines prior to using social media (including Firm operated social media) while an employee of the Firm.

Employees should be aware that while not always apparent, work-related issues may often be implicated by their use of social media. In all instances, employees are expected to use good judgment and to consider the effect their social media use has on others and the way in which others perceive them. Stay Legal – Employees should make sure that their use of social media complies with all applicable laws. When in doubt, the employee should find out whether what he/she is doing is legal before proceeding.

Confidentiality – An employee's confidentiality obligations extend to his/her online activities. Accordingly, employees should be familiar with the Firm's policies regarding confidential information. Generally speaking, an employee should not disclose to any third party any information related to the Firm or its employees, products, services, clients, partners, suppliers, or other business interests unless that information is already public knowledge.

Even if the information is public, an employee should avoid discussing the Firm's clients, suppliers, and partners without their permission. If in doubt

about whether particular information may be disclosed, contact a Managing Partner. Copyrights, Trademarks, and Intellectual Property – Employees should not make any use or reproduction of any copyright, trademark, or intellectual property belonging to any other person or entity, except in accordance with applicable law. NO EXPECTATION OF PRIVACY

Firm employees should have no expectation of privacy withrespectto any information created, viewed, distributed, received, uploaded, downloaded, accessed, or otherwise facilitated by the Firm's Computer or Information Systems (phone, computer, hand-held devices, etc.). Similarly, employees should have no expectation of privacy with respect to information that is generally available online. The Firm reserves the right to monitor and maintain any content created, viewed, distributed, received, uploaded, downloaded, accessed, or otherwise involving any Firm Computer or Information System or resource.

DISCIPLINARY ACTION Any violation of this policy may result in disciplinary action, up to and including termination of employment. Internet Policy For those employees who are provided access to the internet, the Firm encourages the use of the internet for business purposes. Non-business use (such as net surfing for personal enjoyment, entertainment, or children's school projects) should be kept to a minimum and generally restricted to non-working time. Personal use of the internet that adversely affects an employee's productivity is prohibited.

No employee may use the internet during working time or during non-working time to access or convey information in violation of any Firm policy. Examples of the types of information that would violate Firm policies include

information that is sexually explicit or offensive, or which is offensive, hostile, or harassing with respect to anyone's race, religion, color, creed, marital status, sex, ancestry, national origin, age, disability, sexual orientation or preference, veteran's status, or any other aspect that is protected by law or by the Firm's policies.

No employee may use the internet during working or non-working time to access or convey information in an unlawful manner or for any unlawful purpose, such as downloading or copying information or programs in violation of copyright and software licensing laws, or using the internet to distribute or receive destructive programs such as viruses. Remember that you should not expect any " privacy" in your use of the internet.

The Firm has the ability to monitor your internet access (all messages sent, sites accessed, and information downloaded). The Firm reserves the right to review and disclose such records or information with or without prior notice or consent. Your hard drive contains a history of sites recently visited and information (such as text and graphics) from those sites. This information is the Firm's property.

The Firm has the right to enter your workstation or office, with or without notice or consent, at any time, and to access, monitor, review and take possession of your hard drive and any data storage medium. (For example, hard drives, floppy disks, CD-ROMs, videotapes, cassette tapes, etc.) Anything on Company premises is presumed to be Company property and is covered by this policy. I hope this proposal meets all of your contractual needs and gets everyone on the same page. Thank you.