Remote access standards for richman investments essay sample

Law, Security

This document is designed to provide definition of the standards for connecting remotely to Richman Investments' network outside of the company's direct network connection. The standards defined here are designed to mitigate exposure to potential damage to Richman Investments' network, resulting from the use of unauthorized use of network resources. Scope:

All Richman Investments agents, vendors, contractors, and employees, who use either Richman Investments company property or their own personal property to connect to the Richman Investments network, are governed by this policy. The scope of this policy covers remote connections, used to access or do work on behalf of Richman Investments, including, but not limited to, the viewing or sending of e-mail, and the viewing of intranet resources. Policy:

Richman Investments agents, vendors, contractors, and employees with privilege to remote access to Richman Investments' corporate network are responsible for ensuring that they adhere to these standards, whether using company-owned or personal equipment for data access, and that they follow the same guidelines that would be followed for on-site connections to the Richman Investments network. General access to the Internet by household members via the Richman Investments network will not be permitted, and should be used responsibly, such that all Richman Investments standards and guidelines are enforced for the duration of Internet activity. The Richman Investments agent, vendor, contractor, or employee will bear any responsibilities and consequences for any misused access. 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 Richman Investments authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Richman Investments - 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. System and Network Activities The following activities are strictly prohibited, with no exceptions: 1. 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 Richman Investments.

2. 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 Richman Investments or the end user does not have an active license is strictly prohibited. 3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate

management should be consulted prior to export of any material that is in question. 4. Introduction of malicious programs into the network or server (e. g., viruses, worms, Trojan horses, e-mail bombs, etc.). 5. 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.

6. Using a Richman Investments computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. 7. Making fraudulent offers of products, items, or services originating from any Richman Investments account. 8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties. 9. 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. 10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

11. 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. 12. Circumventing user authentication or

security of any host, network or account. 13. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack). 14. 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/Extranet. 15. Providing information about, or lists of, Richman Investments employees to parties outside Richman Investments. Email and Communications Activities

1. 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). 2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages. 3. Unauthorized use, or forging, of email header information. 4. 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. 5. Creating or forwarding “ chain letters”, “ Ponzi” or other “ pyramid” schemes of any type. 6. Use of unsolicited email originating from within Richman Investment’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Richman Investments or connected via Richman Investment’s network. 7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam). (Sans Insitute, 2006) Requirements:

* Remote access must be secure and strictly controlled. Enforcement of control will be via password authentication or private/public keys with strong

pass-phrases. * Richman Investments employees will not, provide their security password(s) to anyone regardless of position. *Richman Investments employees will secure their workstations any time he/she leaves the workstation. *Any Remote User will properly terminate the remote connection, when his/her work is complete, or at the end of the work day. * Richman Investments employees will use the approved Anti-Virus, Anti-Malware and Anti-Spyware programs on a regular basis.

References

City of Lathrop. (2011). City of Lathrop Acceptable Use Policy. Lathrop: City Of Lathrop. Jacobs Engineering Group. (2012). JEG Acceptable Use Policy. Sacramento: Jacobs Engineering Group INC. Sans Insitute. (2006). Acceptable Use Policy. Retrieved from http://www. sans. org: http://www. sans. org/security-resources/policies/Acceptable_Use_Policy. pdf