

APPENDIX A – SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Cornerstone Behavioral Healthcare, LLC (CBH) Security Awareness and Acceptable Use Policy

Overview

The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. CBH is committed to protecting all employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of CBH. 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.

Effective security is a team effort involving the participation and support of every CBH 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.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CBH. These rules are in place to protect the employees and CBH. Inappropriate use exposes CBH to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at CBH, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CBH.

Policy

General Use and Ownership

1. While network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of CBH. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to CBH.
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/Extranet 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.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within CBH may monitor equipment, systems and network traffic at any time.
5. CBH reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: credit card information, company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed every 90 days.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or locking (control-alt-delete for Windows users) when the host will be unattended.
5. Use encryption of information in compliance with Information Technologies' Security Policies.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the corporate security standards, including personal firewalls.
7. Postings by employees from a CBH email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CBH, unless posting is in the course of business duties.
8. All hosts used by the employee that are connected to the CBH Internet/Intranet/Extranet, whether owned by the employee or CBH, shall be continually executing approved virus-scanning software with a current virus database.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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 CBH authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CBH-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 CBH.
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 CBH or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all CBH properties is 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 CBH 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 CBH 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 IT 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, CBH employees to parties outside CBH.

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 CBH's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CBH or connected via CBH's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

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

Definitions

Spam Unauthorized and/or unsolicited electronic mass mailings.

Donna M. Roble

Employee / Contractor / Third Party Signature

11-27-12

Date

DONNA M. ROBLE

Printed Name

11-21-12

Date of Security Awareness Training