Brighton Securities User's IT use and Cybersecurity Document.

Table of Contents:

Part 1: Computer Use guidelines..... 3-6

Part 2: Computer hygiene and best use practices:..... 7

Part 3: Password Procedure:..... 8

Part 4: Bring your Own Device (BYOD) Standards:..... 9

Part 5: Cybersecurity starts with you: 10

Part 1: Computer Use Guidelines:

Overview

Brighton Securities intentions for publishing an Acceptable Use Policy are not to impose restrictions contrary to our established culture of openness, trust, and integrity. The firm is committed to protecting our employees, clients, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The purpose of this policy is to outline the standard acceptable use of computer equipment.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of Brighton Securities. These systems are to be used for business purposes in serving interests of our clients in the course of normal operations.

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.

1.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the firm, including all personnel affiliated with third parties; all equipment that is owned or leased, workstations used to connect to our network, including reading or sending email and viewing intranet web resources.

2.0 Policy

2.1 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 the firm and cannot guarantee confidentiality of information stored on any network device belonging to the firm.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. For security and network maintenance purposes, authorized individuals may monitor equipment, systems, and network traffic at any time.

2.2 Remote Access Requirements

1. Anyone with remote access privileges to the firm's corporate network must not use non-Brighton Securities email accounts (i.e. Hotmail, Yahoo, Gmail, etc.), or other external resources to conduct firm business.

2. Anyone with remote access privileges must ensure that any computer, which is remotely connect to the firm's network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

3. The Brighton Securities employee is responsible to ensure the family member or others do not violate any firm policies, do not perform illegal activities, and do not use the access for outside business interests. The Brighton Securities employee or contractor bears responsibility for the consequences should the access be misused.

4. All Computers that are connected to the firm's Internet/Intranet shall be continually executing approved virus-scanning software with a current virus database.

3.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of Brighton Securities authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing the firm's 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.

4.0 System and Network Activities

The following activities are, in general, prohibited, with no exceptions:

1. Violations of the rights of any person or company protected copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirate" or other software products that are not appropriately licensed for use by the firm.
2. Unauthorized copying of copyrighted software for which the firm or the but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and installation of any copyrighted software for which the firm or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc…).
4. Revealing your account passwords to unauthorized persons or allowing use of your accounts by unauthorized persons. This includes family and other household members when work is being done at home.
5. Using a firm's computing asset to actively in engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws is the user's local jurisdiction.
6. Effecting security breaches or disruptions of network communication. Security breahes 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 expressing authorized to access, unless these duties are within scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of services, and forged routing information for malicious purposes.

7. Port scanning or security scanning is expressly prohibited unless prior notification to the Systems Manager is made.
8. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is part of the employee’s normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
11. 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.
12. Providing information, or lists of, Brighton Securities employees or clients outside the firm.

5.0 Email and Communications Activities.

The following activities are strictly prohibited, with no exceptions:

1. Any form of harassment via email, telephone, paging, or instant messaging, whether through language or frequency and/or size of messages.
2. Unauthorized use, or forging, of email header information.
3. 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.
4. Creating or forwarding “chain letters”; “Ponzi” or other “pyramid” schemes of any type.
5. Use of any email service other than Brighton Securities email to conduct business is strictly prohibited. Email services such as Hotmail, Gmail, and Yahoo are blocked and cannot be used.

Note: All Email, Twitter, LinkedIn, and IM activity is monitored by our archiving software.

6.0 Games

All Microsoft games have been blocked and are prohibited. As stated previously under section “3.1 General Use and Ownership”, employees are responsible for exercising good judgment regarding the reasonableness of personal use. This applies to all other Internet games.

7.0 Enforcement

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

Part 2: Computer hygiene and best use practices:

1. **Please lock your computer whenever you step away from your PC. There are visitors and repair people who come into the building and we want to ensure client data is safe. To lock your computer easily, hold the "windows" key and the "L" key on your keyboard at the same time, this will lock your computer. To log back on, hit "ctrl+alt+del" and then log in with your Network credentials.**
2. There are sites that are blocked, i.e.; gambling, webmail (as per FTC guidelines), pornography, and torrent sites. Please be advised that company internet is to be used for business purposes. (See the Internet use documentation for more details)
3. If you are trying to get to a site and it is blocked, please see IT.
4. We are running Internet Explorer 11 on our machines as the default web browser. This is because Smart Station 2.0 requires it to function properly. If you need a separate browser, please let IT know.
5. Please be careful when clicking links from emails, especially from those coming from outside the company. If you have a question about a link or suspicious email, please contact IT.
6. Please make sure that if you have printed off client information and it is not secured, that you dispose of it in a shred container.
7. USB or external hard drive use is forbidden and locked out by group policy, if you need to get something off of a thumb drive, please see IT.
8. Make sure you are saving personal documents or work on your H Drive.
9. There are two wireless networks here. BSC_Guest for visitors, and BSC_TEAM for employees. Please let IT know if you will need to access to either.
10. When you leave for the day, please log off so that your CPU can automatically download updates overnight. Please restart CPU Friday afternoons to ensure optimal performance.
11. **Make sure to send any password updates to IT as they become available.**

Part 3: Password Procedure:

Overview: There are a lot of password interfaces which allow us to do our daily work here at Brighton Securities. To better serve you, the user, we want to review how passwords are to be handled at Brighton Securities.

1. When you update your Windows, Smart Station, or Global Relay password, please let IT know via an encrypted email/IM/Phone Call/Or in person. Please refrain sending via normal email.
2. When making passwords, make sure to make them complex and hard to guess. Things to avoid include consecutive digits (Ex. 1234), repeating digits (3333), or easily guessed words (Ex. Password/Brighton/Monroe/Fall/Winter/Spring/Summer).
3. Please don't share your passwords with others.
4. Please refrain from keeping your password written down, especially near your desk.
5. If a system has security questions, make sure you remember your security questions as IT will not retain them.

Part 4: Bring your Own Device (BYOD) Standards:

Overview: We as a company feel that being able to use your mobile device allows you a comfort that requiring company issued devices seems to lack. The guidelines below will reflect on how to keep your device in good shape when working at Brighton Securities.

1. You may bring your own mobile device into the building and connect it to the WIFI.
2. You can put work email onto your mobile device. If you need help doing so, please see IT.
3. You can set up your device for remote work. Please see IT for help doing so.
4. It is your responsibility to keep your device healthy. IT recommends installing an antivirus and antimalware app onto your device. See IT for help or suggestions if needed.
5. If your device is on the wifi and it is infected, it will be quarantined. It is the user's responsibility to seek out IT if their device has been quarantined. A quarantined device will no longer connect to our wifi networks until IT has cleared it for return.
6. The Computer use policy applies to your device as long as you are using it on the Brighton Securities' wifi networks.
7. It is recommended to keep your device's operating system updated. This will help with security patches to reduce the risk of infection. If you have any questions, please see IT.

Part 5: Cybersecurity starts with you:

Overview: The new IT landscape requires users to be ever aware of the dangers out there on the internet. This is a new paradigm for your work life. Cybersecurity is just something we will be working with from now on. Working together as a team and by following these guidelines, we can help keep Brighton Securities safe from attack.

1. If you see something, say something: Communication is key to protecting against a cyber attack. If you get a weird phone call or email, report it first. You are NOT wasting IT's time by reporting these. It is better to be safe than sorry in this case.
2. This also includes visitors in the building. If you haven't seen anyone before you see them looking around, you can always engage them. If their answer doesn't seem right, tell IT or management right away. **Always be sure you know what is on a device if you plug it into a computer.** If there is doubt, always see IT first.
3. Not only visitors, but this principle can be applied to items laying around or issues with access. Whether it is someone's keys laying around, to a mystery USB drive laying around, to a door open that should be closed, if it doesn't seem right or you see something like this, alert IT or management.
4. Make sure that documentation with client/employee information is either in your sight, locked away, or in the shred bins when completed. It should not be out for everyone to see.
5. Along with the above, make sure that you don't have any credentials written down near your desk. This is the easiest way for someone to get into your PC and our network.
6. We continue to take steps to secure the building for client/employee safety with locked doors. If you are entering a locked door, make sure that you can absolutely verify that the person who is coming in the door with you is allowed in the building. Tailgating is a form of social engineering which plays on our nature to help people. We keep the main doors open during business hours so we can funnel outside personnel and clients for a reason.

I acknowledge that I have read and understand the items and guidelines outlined in this document. I will abide by them as well.

Name:_____

Signature:_____

Date:_____