Marshall Eddy

CS331-001

Vincent Skimmer

14 November 2016

Information Security Standards

Here is an acceptable use policy from my father’s company, however to keep the privacy of his company…well, private I will replace the company’s name with [company].

**1. PURPOSE**

The purpose of this policy is to outline the acceptable use of [company], Inc ([COMPANY]) computing assets. These rules are in place to protect [COMPANY] employees and the company. Inappropriate use exposes [COMPANY] and its employees to unnecessary risks including malware attacks, compromise of network systems and services, and possible legal, compliance, and regulatory issues.

**2. SCOPE**

This policy applies to all users (including full-time, part-time, and temporary employees, contractors and vendors) of [company], Inc. computing assets including physical assets such as computers, tablets, and smartphones, as well as infrastructure assets including servers, internet access, and networking resources.

**3. POLICY**

**3.1. Overview**

3.1.1. [company], Inc. ([COMPANY]) is committed to protecting itself from illegal and damaging actions through intentional and unintentional means.

3.1.2. [COMPANY] provided computing assets are only provided for conducting work-related activities for a business need.

3.1.3. Each employee is responsible for reading, understanding, and conducting their activities in compliance with this policy.

**3.2. Use, Awareness, and Privacy**  
3.2.1. The [COMPANY] IT Department may conduct audits and/or investigations on [COMPANY] computing assets to ensure compliance with this policy, regulatory guidelines, and any local, state, or federal laws as applicable.

3.2.2. Nothing in this policy will change the legal status of confidential, privileged, or otherwise legally protected information.

3.2.3. Users should be aware that any data created on [COMPANY] computing assets is the property of [COMPANY], unless legal ownership is defined elsewhere by law, such as with confidential or privileged information.

3.2.4. By utilizing [COMPANY] computing assets, all employees acknowledge that there is no personal right of privacy on the computing asset. The use of passwords does not create a right to privacy.

3.2.5. Explicitly authorized individuals within the [COMPANY] IT Department may monitor equipment, systems, and network traffic at any time for security, network, and policy compliance purposes, to include but not limited to E-mail, computer files, and internet usage, with or without notice, at any time, at the company’s discretion. [COMPANY] reserves the right to access and disclose such communications and recordings to third parties under certain circumstances.

**3.3. Security and Proprietary Information**

3.3.1. Information contained on any network or system may be classified as either confidential or public, as defined by organizational confidentiality guidelines. Examples of confidential information include, but are not limited to: medical information, personnel information, user data, vendor and bidder sensitive information, specifications, and other data. Users should take all necessary steps to prevent unauthorized access to this information.

3.3.2. By reading this policy, [COMPANY] employees acknowledge that he or she is responsible for:

3.3.2.1. The security of their own sessions by locking their computers when leaving their workstation.

3.3.2.2. Not sharing passwords for their domain accounts, E-mail, remote access credentials, or any other password protected [COMPANY] resource.

3.3.2.3. Adhering to all policies listed in Section 4: Related Policies.

3.3.2.4. Taking reasonable measures to ensure their laptop computer and mobile devices are protected from theft by not leaving them in exposed locations such as but not limited to: conference rooms, hotel lobbies, and unlocked vehicles.

3.3.2.5. Taking reasonable measures to prevent unauthorized software from installing and/or running on his or her system. All software will be installed by a [COMPANY] I.T. Department technician.

3.3.2.6. Connecting to non-company networks, including other businesses, public or open Wi-Fi, and hotel internet is potentially unsafe and should be limited. Foreign networks are susceptible to snooping, malicious access points, Man-in-the-Middle Attacks.

3.3.2.7. Use of public networks not owned or controlled by [COMPANY] while on a [COMPANY] computing asset must employ the use of a Virtual Private Network (VPN) when conducting business related tasks.

3.3.2.8. Documents that require the ability to be recovered if accidental or otherwise deletion occurs, must be saved to the user’s “H:” drive on the user’s computer whenever possible.

3.3.3. Recommended Security Technologies

3.3.3.1. Password-protected screensavers or lock screens must automatically activate at 15 minutes or less of inactivity on all desktops, laptops, mobile devices, and endpoints.

3.3.3.2. Portable devices including smartphones and tablets that have access to [COMPANY] data or networks must use a PIN or other security feature such passcodes or biometric authentications mechanisms.

3.3.3.3. It is recommended that all users log off their workstations if the device will be unattended for an extended period of time.

3.3.4. Information contained on portable computers and devices is especially vulnerable to data loss through left or losing the device. Special care in the handling, storage, and transportation of this equipment must be exercised.

3.3.5. Loss of any [COMPANY] computing asset by any means must be reported to the [COMPANY] IT Department within 12 hours.

**3.4. Electronic Mail**

3.4.1. Incoming, outgoing and internal Electronic Mail (E-mail) is actively monitored for the transmission of sensitive credit card information, Personally Identifiable Information such as Social Security Numbers, and suspected malware. Any identified E-mail may be opened and read by authorized personnel in the [COMPANY] IT Department.

3.4.2. All E-mail traverses through messaging gateways in order to identify and clean or remove suspected malicious E-mails. A notification of any actions taken by the messaging gateway will be sent to the recipient.

3.4.3. Employees should not open any E-mail attachments that are suspicious, from unknown senders, or otherwise appear malicious. These E-mails should be forwarded to the [COMPANY] IT Department for analysis.

3.4.4. All [COMPANY] E-mails are copied and archived in nearly real-time. Archived E-mails cannot be deleted by users.

3.4.5. Upon employee termination, access to the employee’s mailbox may be granted to other individuals as authorized.

3.4.6. Credentials for accessing one’s E-mail may not be shared with other employees. If a different employee needs access to an employee E-mail while he or she is away from work, the IT Department may set up E-mail forwarding or alternate permissions on the mailbox while the employee is away.

3.4.7. Any form of harassment, sending of unsolicited messages, or creating or forwarding chain letters is prohibited.

3.4.8. Any attempt at modifying or forging E-mail headers or components of the header, including the From address, Reply-To address or Date is prohibited.

**3.5. Instant Messaging**

3.5.1. The use of Instant Messaging (IM) between [COMPANY] employees on [COMPANY] computing assets is permitted.

3.5.2. The use of IM between [COMPANY] employees on [COMPANY] computing assets and non-[COMPANY] employees for work-related tasks is permitted.

3.5.3. The use of IM between [COMPANY] employees and non-[COMPANY] employees for non-work related tasks is not permitted unless explicitly authorized by department supervisors.

3.5.4. Many IM protocols are not encrypted or protected in any way and as such, no confidential, personal, or proprietary information including sensitive credit card information, social security numbers, or employee information may be sent over IM under any circumstances.

3.5.5. Many IM programs retain chat logs on computing assets which may be read by authorized personnel at any time for the purpose of ensuring compliance with this policy.

3.5.6. IM may not be used in any circumstance where there is a policy outlining the requirement to preserve communications.

**3.6. Unacceptable Use**

3.6.1. The following activities are prohibited. This list is not exhaustive but provides a framework for activities that fall into the category of unacceptable use.

3.6.1.1. Any actions that violate U.S., State, Local, or County laws, or [COMPANY] policies.

3.6.1.2. Violations of the rights of any other entity protected by laws or regulations, including but not limited to, the installation or distribution of pirated data, media, or software not appropriately licensed for use by [COMPANY].

3.6.1.3. Installation of any software on computer assets owned by [COMPANY]. Any software required to be installed on an asset must be done so by or approved by the [COMPANY] I.T. Department.

3.6.1.4. Installation of any software owned by or licensed to [COMPANY] on a non-[COMPANY] computing asset without the explicit permission of the [COMPANY] I.T. Department.

3.6.1.5. Unauthorized copying, digitization of, or distribution of copyrighted material, including but not limited to photographs, books, magazines, music, or other copyrighted material for which [COMPANY] or the user does not have an active license.

3.6.1.6. Streaming and/or storage of audio, video, or personal files not related to company business.

3.6.1.7. Utilizing [COMPANY] computing assets or the purposes of conducting a private commercial enterprise or for “moonlighting” purposes.

3.6.1.8. Accessing any data, servers, or accounts for any reason not directly related to and required for the employee’s normal work duties.

3.6.1.9. Introduction of malicious programs or code into the network, servers, or endpoints, including but not limited to viruses, worms, Trojan horses, or time bombs

3.6.1.10. Revealing account passwords for business systems or networks to others or allowing other users to access and use your accounts.

3.6.1.11. Accessing any other employee’s accounts, email, voice mail, files, or other data without explicit permission from the user and the [COMPANY] I.T. Department

3.6.1.12. Using [COMPANY] computing assets to engage in violations of sexual harassment or hostile workplace policies or laws including but not limited to viewing or transferring obscene, pornographic, abusive, slanderous, threatening, and/or offensive material.

3.6.1.13. Executing any form of network or system monitoring which will intercept data not intended for the employee or the employee’s host system, unless this activity is explicitly part of an employee’s normal job duties.

3.6.1.14. The use of USB or other removable media drives not provided by the [COMPANY] I.T. Department is prohibited.

3.6.1.15. Any attempt to circumvent security protection mechanisms on [COMPANY] computing assets including hosts, servers, networks, and accounts.

3.6.1.16. Interfering with or denying service to any other computing system or network other than the employee’s host computer.

3.6.1.17. Any other use of [COMPANY] computing assets for reasons deemed and approved as inappropriate by a [COMPANY] employee’s manager or management team.

**4. RELATED POLICIES, PROCEDURES, AND GUIDELINES**

Bring Your Own Device Policy

Data Protection Policy

Incident Report Procedure

Laptop Usage Standards

Mobile Device Management Policy

Network and Data Access Policy

Password Policy

Password Construction Guidelines

Physical Security Policy

Social Media Standards

Usage Monitoring Policy

Wireless Network Use and Security Policy

References

My Father’s Company’s Acceptable Use Policy