Acceptable Use Policy

Overview

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. MePush is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. MePush does not assume any liability or responsibility for the actions of <Company Name>, nor its employees, partners, subcontractors, or customers.

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 <Company Name>. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> 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 <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct <Company Name> business or interact with internal networks and business systems, whether owned or leased by <Company Name>, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at <Company Name> and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with <Company Name> policies and standards, and local laws and regulation. Exceptions to this policy are documented in the *Policy Compliance* section.

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

Policy

General Use and Ownership

1. <Company Name> proprietary information stored on electronic and computing devices whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of <Company Name> proprietary information.
3. You may access, use or share <Company Name> proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
4. 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.
5. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time.
6. <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. All access to devices and systems are restricted based on job role need to know.
2. All access is limited to the least privileges required to perform the job responsibilities.
3. All access is assigned to an individual based on their job classification and function.
4. All workforce members with access to the EPHI environment will have unique user ID’s and passwords.
5. Sharing of user ID’s or passwords is strictly prohibited.
6. Any remote access is only allowed through 2-Factor Authentication.
7. An Automated Access Control System must be implemented for all system components and
8. must be set to a ‘deny all’ default setting.
9. System level and user level passwords must comply with the password policy below.
10. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
11. Password Policy:
    a. Passwords will be protected by strong cryptography during transmission and storage on all system components.
    b. Passwords must follow best practices for password length and complexity, while being changed on a regular basis.
    c. Passwords must never be written down.
    d. Passwords must never be shared with anyone.

e. All non face-to- face password reset requests for Workforce Members with access to the EPHI environment require verification of the Workforce Members identity.
f. All first time passwords for Workforce Members with access to the EPHI environment must be set to a unique value and must be changed after the first use.
g. The use of group or shared User ID's or passwords is strictly prohibited.
h. All passwords must:
    i. Be changed at least every 90 days.
    ii. Be at least 8 characters in length.
    iii. Contain both numeric and alphabetic characters.
    iv. Be different than the previous four passwords.
    v. Be re-entered if the session has been idle for more than 10 minutes.

12. System access accounts of terminated Workforce Members must be deactivated or removed immediately. All inactive or disabled user accounts must be removed at least every 90 days.
13. Vendor accounts for remote or on-site maintenance are only enabled during the time period needed by the vendor.
14. <Company Name> will monitor all vendor access during use.
15. Functions for each workstation or class of workstations are defined along with approved locations for use of the workstation.
16. All computing devices must automatically log off or must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
17. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
18. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

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 <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-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 <Company Name>.
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 <Company Name> or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting <Company Name> business, even if you have authorized access, is prohibited.
4. 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.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. 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.
7. Using a <Company Name> 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.
8. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. 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.
11. Port scanning or security scanning is expressly prohibited unless prior notification to MePush is made.
12. 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.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the <Company Name> network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. 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.

17. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to the IT Department.

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

Blogging and Social Media

1. Blogging by employees, whether using <Company Name>’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>’s policy, is not detrimental to <Company Name>’s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>’s systems is also subject to monitoring.
2. <Company Name>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>’s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>’s Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in

blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Compliance Measurement

The compliance team at <Company Name> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the <Company Name> senior management or the IT Department (MePush) in advance.

Non-Compliance

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

Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

Definitions and Terms

Terms can be found in the sites located at:

https://www.sans.org/security-resources/glossary-of-terms/

https://www.pcisecuritystandards.org/pci_security/glossary/

https://www.hhs.gov/hipaa/

More terms:

- Access refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
- Access Control provides users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files and should enable authorized users

to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that <Company Name> deems appropriate.

- Automated Access Control System refers to an authentication system, such as Windows Active Directory or Windows Username and password authentication, which requires that the Workforce Member enter in their own unique username and password.
- EPHI Environment is composed of all computer systems and components which transmit, process, access, maintain or store Electronic Protected Health Information (EPHI).
- Protected Health Information (PHI) refers to any data that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). Also EPHI for Electronic Protected Health Information.
- Workforce refers to faculty, staff, volunteers, trainees, students, agents, and other persons whose conduct, in the performance of work for <Company Name>, is under the direct control of <Company Name>, whether or not <Company Name> pays them.
- Workstation refers to all electronic computing devices, for example a laptop, desktop, smart phone, tablet computer or any other device that performs similar functions. It also includes any electronic media stored in its immediate environment. This means that in addition to the devices, flash drives, USB drives or any other attached or removable media is included.
- 2-Factor Authentication consists of using at least two of the following three items to log in to a system or gain physical access to an area. Using 2-factor authentication greatly increases the security of the system, particularly from Internet based attacks:
- Something you know – Examples are Username and password or answers to security challenge questions
- Something you have – Examples are an RSA token or a cell phone which generates or receives time sensitive one-time codes
- Something you are – Examples are fingerprint scanner or iris scanner

Sources

- **SANS**: Text from this policy was primarily sourced from SANS, the authority on Internet Security. SANS Consensus Policy Resource Community Acceptable Use Policy: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy
- **SecurityMetrics**: HIPAA portions were sourced with permission from Workstation Use and Security Policy by SecurityMetrics, Inc.

Agreement

I have read and agree with the above policy.

Name: _____ Signed: _____ Dated: __/__/____