Internet Security Policy

Purpose

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of BenefitHelp information and equipment by Internet connections.

Scope

This policy applies to all employees, contractors, consultants, temporaries, and other users at BenefitHelp, including those users affiliated with third parties who access BenefitHelp computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by BenefitHelp.

Specific policy

All information traveling over BenefitHelp computer networks that has not been specifically identified as the property of other parties will be treated as though it is a BenefitHelp corporate asset. It is the policy of BenefitHelp to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of BenefitHelp to protect information belonging to third parties that has been entrusted to BenefitHelp in confidence as well as in accordance with applicable contracts and industry standards.

Introduction

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes BenefitHelp's official policy regarding Internet security. It applies to all users (employees, contractors, temporaries, etc.) who use the Internet with BenefitHelp computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with BenefitHelp.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the Chief Technology Officer (CTO). Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

Information movement

All software downloaded from non-BenefitHelp sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with BenefitHelp information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal BenefitHelp information (see the following section).

Users must not place BenefitHelp material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the director of marketing or president has first approved the posting of these materials.

In more general terms, BenefitHelp internal information should not be placed in any location, on machines connected to BenefitHelp internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writable (common/public) directories on BenefitHelp Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with BenefitHelp's business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

Information protection

Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, BenefitHelp secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by the BenefitHelp Chief Technology Officer (CTO), must be used to protect these parameters as they traverse the Internet.

This policy does not apply when logging into the machine that provides Internet services. Currently BenefitHelp does not use any type of encryption.

In keeping with the confidentiality agreements signed by all staff, BenefitHelp software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-BenefitHelp party for any purposes other than business purposes expressly authorized by management.

Exchanges of software and/or data between BenefitHelp and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

Regular business practices, such as shipment of software in response to a customer purchase order, need not involve such a specific agreement since the terms are implied.

BenefitHelp strongly supports strict adherence to software vendors' license agreements. When at work, or when BenefitHelp computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with BenefitHelp work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

Expectation of privacy

Staff using BenefitHelp information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.

At any time and without prior notice, BenefitHelp management reserves the right to examine e-mail, personal file directories, and other information stored on BenefitHelp computers. This examination

assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of BenefitHelp information systems.

Resource usage

BenefitHelp management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, time. Likewise, games, news groups, and other non-business activities must be performed on personal, not company, time.

Use of BenefitHelp computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is preempted by the personal use. Extended use of these resources requires prior written approval by a Senior Manager.

Public representations

Staff may indicate their affiliation with BenefitHelp in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In either case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, or not necessarily those of BenefitHelp.

All external representations on behalf of the company must first be cleared with the director of marketing or president. Additionally, to avoid libel problems, whenever any affiliation with BenefitHelp is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

Staff must not publicly disclose internal BenefitHelp information via the Internet that may adversely affect BenefitHelp’s customer relations or public image unless the approval of the CEO has first been obtained. Such information includes business prospects, unit costing, RFP information, and the like. Responses to specific customer e-mail messages are exempted from this policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If staff are not careful they may let the competition know that certain internal projects are underway. If a user is working on an unannounced product, a research and development project, or related confidential BenefitHelp matters, all related postings must be cleared with one's Senior Manager prior to being placed in a public spot on the Internet.

Access control

All users wishing to establish a connection with BenefitHelp computers via the Internet must authenticate themselves at a firewall before gaining access to BenefitHelp's internal network. This authentication process must be done via a dynamic password system approved by the Chief Technology Officer (CTO).

Examples are handheld smart cards or user-transparent challenge/response. This will prevent intruders from guessing passwords or from replaying a password captured via a "sniffer attack" (wiretap). Designated "public" systems do not need these authentication processes because anonymous interactions are expected. Currently, BenefitHelp does not use this system.

Unless the prior approval of the CTO has been obtained, staff may not establish Internet or other external network connections that could allow non-BenefitHelp users to gain access to BenefitHelp systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet home pages, FTP servers, and the like.

Likewise, unless the CTO, CMO, CEO, and legal counsel have all approved the practice in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

Reporting security problems

If sensitive BenefitHelp information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the CTO must be notified immediately.

If any unauthorized use of BenefitHelp information systems has taken place, or is suspected of taking place, the CTO must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the CTO must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not "test the doors" (probe) security mechanisms at either BenefitHelp or other Internet sites unless they have first obtained permission from the CTO. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

Responsibilities

As defined below, BenefitHelp groups and staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

a) Information Systems must establish Internet security policies and standards and provide technical guidance on PC security to all BenefitHelp staff. The IT department must also organize a computer emergency response team (CERT) to respond to virus infestations, hacker intrusions, and similar events. The CERT Team is identified in BenefitHelp Personal Computer Security Policy.

b) IT staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the Internet security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to Internet security.

c) IT staff must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

d) IT staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

e) IT staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.

f) BenefitHelp information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

g) BenefitHelp Senior Management must ensure that:

1. Employees under their supervision implement security measures as defined in this document.
2. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
3. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all BenefitHelp documents that address information security.
4. Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
5. Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

h) Users of BenefitHelp Internet connections must:

1) Know and apply the appropriate BenefitHelp policies and practices pertaining to Internet security.
2) Not permit any unauthorized individual to obtain access to BenefitHelp Internet connections.
3) Not use or permit the use of any unauthorized device in connection with BenefitHelp personal computers.
4) Not use BenefitHelp Internet resources (software/hardware or data) for other than authorized company purposes.
5) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
7) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
8) Report to the CTO or IT staff any incident that appears to compromise the security of BenefitHelp information resources. These include missing data, virus infestations, and unexplained transactions.
9) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
10) Obtain supervisor authorization for any uploading or downloading of information to or from BenefitHelp multi-user information systems if this activity is outside the scope of normal business activities.
11) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their Senior Manager.

Contact point
Questions about this policy may be directed to the CTO.

Disciplinary process
Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

Employees receive copies of the company’s use policies their first day on the job and are given an explanation while meeting the company’s department heads.

Acceptable use policy for Your company office environments

1. Purpose
The Company owns and operates various computer systems, which are provided for use by employees in support of business activities. All users are responsible for seeing that these facilities are used in an effective, ethical and lawful manner.

This document establishes rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions under federal, state or local laws.

2. Audience and agreement
All users of the company's computing systems must read, understand and comply with the policies established in this document as well as additional guidelines established by administrators of each system.

BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

3. Rights

These computer systems, facilities and accounts are owned and operated by BenefitHelp reserves all rights, including termination of service without notice, to the computing resources it owns and operates. These procedures shall not be construed as a waiver of any rights of BenefitHelp, nor shall they conflict with applicable acts of law. Users have rights that may be protected by federal, state and local laws.

4. Privileges

Access and privileges on BenefitHelp computing systems are assigned and managed by the system administrators of specific individual systems. Eligible individuals may become authorized operators of a system and be granted appropriate access and privileges by following the approval steps for that system.

A designee of the IT department must approve all access to BenefitHelp computer resources, including the issuing of passwords.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without permission from the system administrator. The authorized user is responsible for the proper use of the system, including any password protection. Users may not install any device on a computer without authorization from the system administrator.

5. Responsibilities

Users are responsible for maintaining the following:

1. An environment in which all BenefitHelp computing resources are shared equitably among users. The system administrator of each system sets minimum guidelines within which users must conduct their activities. An environment that does not harm the functionality of the equipment.

2. An environment conducive to business:
   A user who harasses, or makes defamatory remarks, shall bear the full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that BenefitHelp's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by BenefitHelp.

   Many of BenefitHelp's computers provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that BenefitHelp does not assume responsibility for the contents of any of these outside networks.

   The user agrees to comply with the acceptable use guidelines presented in this document, and other documents for outside networks or services they may access through BenefitHelp computer systems.

   Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through the system administrators and through specific individual networks.

   The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message, a message that is inconsistent with an environment conducive to business or with a misleading origination, the person who

performed the transmission will be solely accountable for the message, not BenefitHelp, which is acting solely as an information carrier.

3. An environment free of illegal or malicious acts:

   The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which he or she is authorized, or any attempt to deprive other authorized users of resources or access to any BenefitHelp computer system shall be regarded as malicious, and may be treated as an illegal act.

4. A secure environment:

   Any user who finds a possible security lapse on any system is obligated to report it to the system administrators.

   Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.

   Users are responsible for backup of their own data.

6. Accounts

An account assigned to an individual must not be used by others without written permission from the system administrator. The individual is responsible for the proper use of the account, including proper password protection.

7. Confidentiality

While reasonable attempts have been made to ensure the privacy of your accounts and your electronic mail, there is no guarantee that your accounts or electronic mail is private. The systems are not secure nor are they connected to a secure network. It is entirely possible that in the course of normal system administration activities your e-mail, and any data stored in your account, will become visible to the system administrator. Further, in case of a request from law enforcement authorities, your e-mail and other data may be made available to the requesting agency.

8. System usage

Electronic communications facilities (such as e-mail) are for company related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

9. System performance

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any company computer system.

10. Unauthorized access

Loopholes in the computer system or knowledge of a special password should not be used to damage the computer system, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given.

11. Copyright

Computer software protected by copyright is not to be copied from, into, or by using BenefitHelp computing facilities, except as permitted by law or by contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner.

The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

Copyright and licensing restrictions
BenefitHelp abides by all applicable federal and state statutes and regulations pertaining to the use of computer hardware and software including, but not limited to, federal copyright laws. Unauthorized copying, altering, modifying, merging, transferring, de-compiling, or reverse assembly of licensed software is strictly prohibited. Tennessee law further governs the use of any computer resource (including software).

Single CPU usage restrictions
Most copyright licenses for software contain single CPU usage restrictions. These restrictions must be honored. In some instances, the software copyright owner may grant a variance from these restrictions to BenefitHelp. However, without explicit written variance, single usage restrictions in the license apply to all users.

12. Violations
An individual's computer use privileges may be suspended immediately upon discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate supervisors.

Violations of these policies will be dealt with in the same manner as violations to other company policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the company, and legal action. Violations of some of the above policies may constitute a criminal offense.

13. Additional guidelines
System administrators will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowable connect time and disk space, handling of non-retrievable mail, responsibility for account approval and other items related to administrating the system.

E-mail security policy

Purpose
This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

Scope
The policies apply to BenefitHelp employees and contractors and cover e-mail located on BenefitHelp personal computers and servers if these systems are under the jurisdiction and/or ownership of BenefitHelp. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

Specific policy

Company property. As a productivity enhancement tool, BenefitHelp encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of BenefitHelp, and are not the property of users of the electronic communications services.

Authorized usage. BenefitHelp electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

(a) It does not consume more than a trivial amount of resources.

(b) It does not interfere with staff productivity.

(c) It does not preempt any business activity.

Users are forbidden from using BenefitHelp electronic communications systems for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the BenefitHelp president or his representative. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Default privileges. Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a program director has been obtained.

User separation. These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. But fax machines that do not have separate mailboxes for different recipients need not support such user separation. All BenefitHelp staff and authorized contractors have unique usernames and passwords to access the e-mail system.

User accountability. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

No default protection. Employees are reminded that BenefitHelp electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See the Chief Technology Officer (CTO) if this requirement is needed.

Respecting privacy rights. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. BenefitHelp is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, BenefitHelp also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

No guaranteed message privacy. BenefitHelp cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

Regular message monitoring. It is the policy of BenefitHelp NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that BenefitHelp will from time to time examine the content of electronic communications.

Statistical data. Consistent with generally accepted business practice, BenefitHelp collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, IT staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

Incidental disclosure. It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper Senior Management approval channels.

Message forwarding. Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. BenefitHelp sensitive information must not be forwarded to any party outside BenefitHelp without the prior approval of a Senior Manager or the BenefitHelp CEO. Blanket forwarding of messages to parties outside BenefitHelp is prohibited unless the prior permission of the CTO has been obtained.

Purging electronic messages. Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period—generally six months—electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IT staff.

Not only will this increase scarce storage space; it will also simplify record management and related activities. If BenefitHelp is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the BenefitHelp CEO or his designated representative has communicated that it is legal to do so.

Responsibilities

As defined below, BenefitHelp groups and staff members responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.

1. IT must establish e-mail security policies and standards and provide technical guidance on e-mail security to all BenefitHelp staff.
2. IT staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the personal computer security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
3. BenefitHelp Senior Management must ensure that:
    - Employees under their supervision implement e-mail security measures as defined in this document.

Contact point
Questions about this policy may be directed to the CTO.

Disciplinary process
Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

I have read and understand the Internet and Email Security Policies for BenefitHelp.

_____ _____

NAME DATE

_____

SIGNATURE