

**My Company's (XXX)
NETWORK, MESSAGING AND ON-LINE SERVICES
ACCEPTABLE USE GUIDELINES**

CONTENTS:

- 1.0 Acceptable Use
 - 1.1 Electronic Mail
 - 1.2 News Groups
 - 1.3 Other (Internet and dial-up) On-line services
 - 1.4 Personally owned (non-XXX) hardware and software
- 2.0 Password discipline and use
- 3.0 Laptop/Portable Computer security
- 4.0 File Transmission security
- 5.0 Network dial-out and dial-in (Remote Access) security
- 6.0 Closing

1.0 ACCEPTABLE USE GUIDELINES

Some guidelines for acceptable use of specific XXX resources are covered in the following sections:

1.1 ELECTRONIC MAIL

Any electronic mail (e-mail) generated by or between corporate (XXX's) computers on or over our network is the property of XXX and is subject to review at any time. E-mail service is provided to employees by XXX as a means of enhancing the communications, productivity and connectivity of its employees and its use is intended to be of a business nature.

As a convenience to its employees, XXX allows the use of corporate e-mail resources for other than strictly business purposes, but this use is still subject to company review and must be consistent with company policies, prevailing ethical and moral standards and comply with the law of the land. For non-business messages of general interest, offers to sell or buy something or for other non-business related issues, XXX maintains internal news groups to which such items can be posted. For more on news groups see Section 7.0.

Mail should be addressed to the smallest group of recipients possible consistent with getting the job done. Use of the location aliases (XXX_XXX, etc.) and the global alias (XXX_everyone) should be restricted to the absolute minimum necessary to properly communicate the message.

Employees are asked to closely monitor their mail accounts and minimize the amount of mail stored on the mail servers. Mail stored on the mail servers will be

purged after 90 days. Any employees needing to retain mail longer than that period should file the mail in a location that supports longer retention (such as their home folder on the applicable file server). Normal file storage procedures for data volumes retain weekly backups for approximately six weeks, monthly backups for one year and annual backups for three years. Mail server data is backed up and stored separately and is subject to the 90 day limit.

Because of the ephemeral nature of e-mail, attachments that need to be periodically referred to, updated or retained for future use should be separated from the e-mail that carries them and put into the normal document handling system. Currently this document handling system consists of UNIX home directories and consolidated file storage on a common system (CentralNTServer) for PCs, Macs and UNIX machines. This storage system (CENTRALNTSERVER and UNIX home directories) is accessible over the network, and is broken out in home directories by UNIX user ID on Top and Loki and in volumes for public use, by departments, and into home directories by another user ID and password on CentralNTServer. The departmental volumes can be sub-divided into as many directories as necessary to facilitate file storage by group, project, topic etc. Access to directories (file folders) can be controlled by group membership, individual user ID and password, and include read/write or read-only permissions as necessary.

Mail (and its attachments) is maintained in-house and sent (internally or externally) in clear text. That means that anyone that is even minimally sophisticated in network issues can (and does) trap your mail as the packets are transmitted out of our network onto the Internet, and can read your e-mail (and most attachments) just as if they'd been sent to them. Consequently, this isn't a very secure environment to entrust company proprietary or confidential information. If a message containing such information must be sent out, you should first explore available alternatives for encryption and compression (as necessary) of the information and clear the transmission with your department head. For UNIX users the tar procedure supports encryption and compression as does WinZIP™ for PC-compatibles and Stuffit Deluxe™ for Macs. If the person on the destination end of your message is capable of any of these alternatives then their use should be explored. Tar is available on most UNIX machines as a standard utility, WinZIP™ is licensed for use on our PC's, and Stuffit Deluxe™ is a commercial product for Macs. Information Services is currently exploring some user-transparent WAN and Internet encryption alternatives based on Netscape Communicator™, but that is still in the testing phase.

In addition, employees frequently send mail messages with large attachments to internal mail groups, or multiple XXX recipients, some of whom are located at other geographical locations and access their mail over restricted-bandwidth (i.e. small and slow) connections. It is much better in these instances to store the files (attachments) on commonly available file servers such as

CENTRALNTSERVER and reference the locations in the messages instead of attaching the files. That way all can get the message quickly and easily and those who actually need to retrieve the files can do so with minimal impact on the network and other users.

1.2 NEWS GROUPS

News Groups are loosely managed discussions conducted over the Internet or Intranet via e-mail. There are moderated (very loosely) discussion groups and unmoderated groups. Currently XXX carries a sub-set of the moderated groups and over 40 discussion groups internal to XXX. The groups carried by XXX are chosen by content and intended to provide information to employees to aid in their jobs and provide industry information. Some additional news groups are carried for the benefit of employees in their break or non-work time. Providing access to a group discussion does not constitute endorsement of the discussion topics or content, and XXX does not intentionally carry groups whose language, content or topics would be offensive or could in any way cause harm. However, the very nature of the structure of news groups makes them vulnerable to excesses in behavior, belief and language on the part of any of the participants, so be forewarned.

Internal news groups have been established to facilitate the exchange of information between employees. XXX's news groups currently exist on topics such as e-mail, lost & found, the various desktop computing platforms, etc. Groups can be added by request to the help desk at any time, are internal to the company's network (hence relatively secure) and can be used for the dissemination of product information, technical documentation and manuals, and as forums for discussion of future product direction, functionality, interface requirements, and exchange of development information and files. Information exchanged via news groups should be handled similarly to e-mail, with all the cautions, restrictions and guidelines for proper use as outlined above.

1.3 OTHER (INTERNET-ACCESSIBLE AND DIAL-UP) ON-LINE SERVICES

Many other avenues to the Internet and on-line services (such as America On-Line™, etc.) exist and are available for your use. XXX is not concerned with your involvement with these except as it might impact XXX's business operations. If you represent yourself as an employee of XXX or post information on behalf of XXX, regardless of the service used or the user ID under which you are registered or logged in, you must abide by all corporate rules and responsibilities expressed in this document and all other agreements, rules and regulations related to your employment at XXX. Remember that as an employee you are an ambassador for XXX and you are expected to conduct yourself accordingly.

1.4 PERSONALLY OWNED (NON-XXX) HARDWARE AND SOFTWARE

Personally owned software should not be installed on XXX computers. XXX-provided software may be installed on personally owned machines if needed to support work for XXX and if approved by the employee's manager. However, some software licenses don't allow such installation, and those that do place restrictions on its use. Such installation and use must be done in accordance with company policy and applicable software licenses. Personally owned hardware should only be used with the approval of the employee's manager for specific company projects or use. If approved, IS will manage the hardware as they would for XXX systems and in standard XXX configuration. Personal installation and use of non-standard software on such systems will not be supported by IS.

2.0 PASSWORD DISCIPLINE AND USE

Access to company critical, limited distribution and personal information via systems and applications at XXX is controlled by the use of user identification and associated passwords. Each employee is identified by a unique user ID (e.g., xxx2xx1) and access to groups, accounts, files and other restricted use is controlled for this user ID by a confidential, encrypted password. Since access to restricted areas and data is controlled and monitored by use on such a system, employees must not permit any others to access e-mail or other protected applications through their accounts. Temporary access may be granted to IS systems administrators or other company officials as long as the user monitors the use and takes full responsibility for any actions that may result. Users should immediately change their passwords to secure their account after such access.

Currently XXX must use several systems to provide the necessary security for day-to-day operations. (UNIX systems and user account management; Windows NT™ accounts; remote access accounts, and several database access accounts.) This complicates the password and ID process for the users and administrators and results in significant inconvenience and extra work for us all. IS is working toward implementation of a centralized directory structure that will allow control and management of user ID's from the central directory and facilitate single-sign-on procedures for users. When implemented, such a system will greatly simplify IS administration and user maintenance of accounts. Implementation of such a system is at least six months out. IS recommends the following procedures for user account security:

- Change your password at least every 90 days.
- Use at least six characters in your password.
- Use at least one numeric and one non-alpha/numeric character.
(e.g., buffy?1)
- **Don't write down your user ID and password on a yellow sticky note and paste it to your monitor.**
- Don't write down your password anywhere, keep it in your head.
- If you forget your password or are locked out of your accounts, contact the help desk and IS will reset your password to a default and you can log in and change it.
- If you've never changed your password or don't remember how, please contact the help desk and they will assist you.

3.0 LAPTOP/PORTABLE COMPUTER SECURITY

Laptop computers are great tools and can be invaluable productivity enhancers especially for users that travel frequently. However, laptops present some critical management and security issues for XXX and its employees. The chief security issues are:

- loss of a capital asset
- loss of or compromise of confidential company information, documentation, and intellectual property (e.g., company source code)
- compromise of access to protected company data and network resources through loss of control for configured remote access, e-mail and protected database applications

What can we do to guard against this? There are several options available to us. The laptop itself can be protected by commercial applications that password protect the computer and access to its applications and data. We can also, through other commercial applications, encrypt our data and password protect the encrypted files. These measures introduce a significant amount of overhead to the process of using a laptop and add additional chances for data loss through failures in the protection software or loss or corruption of access account ID's or passwords. Such inconveniences pale in comparison to the potential consequences of lost or compromised critical company information. Therefore laptop users and their supervisors should weigh the consequences of the loss of computers and the data contained in them and take appropriate measures to protect the assets and the data. Some suggestions on data protection and laptop security:

- Never carry confidential information on your laptop in an unsecured, unprotected state. Encrypt your confidential files and protect them with a password as a minimum. PC users can use WinZIP™, Mac users can use Stuffit Deluxe™, and UNIX users can use the tar utility to encrypt and password protect their files. This isn't infallible or unbreakable but protects the files from casual or incidental compromise.
- Never "pre-configure" data access applications with your user ID and password and allow the programs to save that data for automatic use next time. For example, many e-mail packages allow you to preset your user ID and password and save them in the program so it can automatically log you in and get your mail the next time its used. That is certainly convenient, but that also means that anyone in possession of your laptop can dial-up our network and log into your e-mail as you and check your mail or send mail as you.
- If your laptop is stolen or you lose it, notify the Help Desk and your supervisor immediately. IS can lock your accounts and block network and data access quickly and will then work with you to re-establish your secure access.

4.0 FILE TRANSMISSION SECURITY

Remember that files transmitted outside XXX's LAN or WAN can be intercepted and, if not protected, can be read at will by virtually anyone with a connection to the Internet. **Therefore, it is vitally important to our secure operations and the protection of our intellectual property that you never transmit outside our internal network (LAN/WAN) confidential files, source code or other elements relative to our products or internal operations without encrypting the files first.** The current mail product, Netscape Communicator™, has the capability to encrypt files in both internationally approved, exportable format and in the "strong encryption" format authorized for use in the U.S. and Canada. In addition, industry standard utilities that support adequate encryption and password protection are available as mentioned in 5.1 above.

5.0 NETWORK DIAL-OUT AND DIAL-IN (REMOTE ACCESS) SECURITY

Dial-out and Dial-in access from and to our internal network is one of the most serious areas of risk to network security in our company today.

Dialing out of our network via modem establishes a direct link between our network and the network on the other end of the connection. This may or may not be a significant security breach, but the point is that you have **no way of knowing the security of the connection you have established.** In order to properly protect against this risk, it is essential that all lines used for outbound modem access be terminated outside our existing firewall. Anyone using outbound modem dialing must notify IS and have their lines or modem access checked for proper security and configured for secure operation if necessary. Failure to do so is grounds for termination.

Dial-in access to our network is protected by user ID and password security. This access is only as secure as the computer, software, user ID and password procedures used by the employee. If you keep a copy of your user ID and password on a sticky note on your laptop screen, then XXX has no effective security no matter what procedures we use to safeguard the system internally. You should exit computer applications when you finish using them. You should never configure applications to contain (automatically) both your user ID and your password. Laptops should be secured by software or hardware and software that restricts the use of the computer to authorized persons in case of loss or theft. Passwords and user ID's should never be "shared" between multiple users.

6.0 CLOSING

Common sense, company policy and the procedures outlined in this document will help to ensure that XXX has a safe, secure and effective computing environment. If you have any questions please contact the IS Department Help Desk or the IS Director.