

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

CONTENTS:

- 1.0 Synopsis
- 2.0 Scope
- 3.0 Expectations
- 4.0 Enforcement of these Policies

1.0 SYNOPSIS

This document defines the criteria for acceptable use of XXX's information services and network resources. In this document these resources are defined as our Intra- and Internet connections, local area network (LAN), and wide-area network (WAN), messaging, and any other on-line services accessed through or using XXX equipment or connections.

2.0 SCOPE

This document governs company policy regarding the use of all Internet, messaging (e-mail), and on-line services, including, but not limited to, America On-line™, CompuServe™, cc:Mail™, MCI-Mail™, SMTP Mail, POP Mail, IMAP-based Mail, UNIX mail, Eudora™ Mail, Netscape/Communicator™ Mail, and other services accessed via XXX communications and computing systems. It also will address basic standards for use of XXX's LAN, WAN, protection of capital and intellectual property, and connections established between our network and the networks of the customers we support. All XXX employees, Officers of the Company, members of the Board of Directors, temporary employees, and contractors are responsible for following the policies set forth in this document.

3.0 EXPECTATIONS

Access to the Internet, Intranet, electronic messaging, and other computer or network based services is provided for business-related use. When using network services at XXX or anywhere on behalf of XXX, it is important to remember that you are a representative of the company and your conduct can have direct impact on it.

Every action you take on the Internet is monitored. There are numerous organizations that specialize in monitoring activity on the Internet. These organizations are aware of which sites you visit, the amount of time you spend at each site, and are able to monitor the types of communication you make with an individual or web site via the Internet. In addition, XXX monitors all in-bound and out-bound Internet activity. When using Internet services, as provided by XXX, you agree to XXX-monitoring of all your Internet communications.

As a representative of XXX, you are expected to use these services in a manner that:

- *effectively uses system resources* (i.e. use FTP rather than e-mail to transfer large files, don't leave Internet or application connections up while away from your system, etc.). Usage levels for services not directly supporting XXX's business will not be allowed to rise to an extent that impedes the company's ability to conduct business appropriately or respond to business need expeditiously.
- *protects against unauthorized use* (i.e. Don't share passwords or read another user's mail). Use passwords to protect your accounts. Use screen locks and log out from your system or applications when away from your desk for extended periods. The display or printing of any kind of sexually explicit image or document on any company system is a violation of XXX's policy on sexual harassment and is grounds for dismissal. XXX reserves the right to explicitly block access to any site it determines unacceptable.
 - *is consistent with XXX's employment and confidentiality requirements.* Transmission of proprietary XXX data using insecure services such as Internet E-mail requires approval by your supervisor and the IS department prior to transmission. Non-Disclosure Agreements are required for all outside parties before the disclosure of XXX confidential or proprietary information. Refer to the XXX Employee Handbook and contact Human Resources for additional information.
 - *honors third-party copyrights and other intellectual property rights.* Much of the software and other material available on the Internet requires payment to the author. Please read all copyright notices and handle such materials in accordance with the requirements contained in the copyright notice.
 - *does not violate any applicable laws and regulations* (domestic and international). XXX's network, Intranet and Internet facilities must not be used to violate any applicable laws or regulations. Any questions regarding legality should be discussed with your supervisor and/or XXX's legal department.
 - *protects against computer worms, viruses, etc.* All files downloaded from the Internet should be scanned by a competent individual using approved virus protection software prior to use or transfer.
 - *protects against monetary loss.* While data encryption techniques are beginning to be used on the Internet, most Internet traffic remains unencrypted. It is, therefore, considered unsafe to transmit account numbers, credit card numbers, etc. over the Internet unless special precautions are observed.

4.0 ENFORCEMENT OF THESE POLICIES

XXX considers any violation of these policies a serious offense. Electronic messages or any other data and software residing on XXX systems are not private, and XXX reserves

the right to copy and/or inspect any data and software on XXX systems. XXX may track Internet usage (e.g., file transfers, connectivity, and web site communications), e-mail activity and application use. In addition you will be held responsible for the consequences of any violation by you of these policies, which may include individual and personal liability for any damage award, as well as responsibility for any crime you may commit while using these types of services, even while using them via access provided by XXX. Lack of knowledge about such violations is not a valid defense in these instances.