INFORMATION TECHNOLOGY SECURITY AND APPROPRIATE USE POLICIES

(INCLUDES INTERNET, EMAIL, AND TELEPHONE)

All XXORGANIZATION employees and consultants must acknowledge receipt of these policies prior to being given a user-ID and/or provided access to XXORGANIZATION systems.

ACKNOWLEDGEMENT

I hereby acknowledge that I have received, reviewed, understand and appreciate the implications of the (attached) *Internet, Email, Telephone, and Information Security Policies*, and by signing (below) I agree to abide by these policies.

Moreover, I hereby acknowledge that these policies supersede all previous oral or written representations, policies, procedures and practices, and that these policies may be amended from time to time. A current copy is posted and available on the XXORGANIZATION Intranet.

Signature: _____ Date: _____

XXXDEPARTMENT
XXORGANIZATION
VERSION:

INTRODUCTION

Information and information systems are critical and important XXORGANIZATION assets. Moreover, new resources, new services, and the "interconnectivity" now available via the Internet introduces not only new opportunities, but new risks as well. Without a doubt, computers and the Internet have changed -- and will continue to change -- the nature of work in our society.

Scope

In response to such risks and requirements the XXORGANIZATION has adopted this policy regarding use of the Internet, Email and overall Information security. It applies to all XXORGANIZATION employees, contractors, temporaries and consultants who use the XXORGANIZATION systems. Questions about this policy and/or any XXXDEPARTMENT should be directed to the XXXPERSON of XXXDEPARTMENT. Violations of these policies can lead to revocation of system privileges and/or disciplinary action including termination.

General

The XXORGANIZATION uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. The XXORGANIZATION disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

PERSONAL FILES AND INFORMATION

Personal files stored on XXORGANIZATION computers and in XXORGANIZATION worker's desks will generally be handled with the same privacy perspective given to personal mail sent from or received at the XXORGANIZATION, and personal phone calls made or received at the XXORGANIZATION.

However, staff should be aware of the following limitations that apply to the privacy of files, documents, email and/or other electronically stored or transmitted materials:

1) By making use of XXORGANIZATION systems, users consent to allow all information they store on any and all systems to be divulged to law enforcement at the discretion of XXORGANIZATION management.

2) All messages, documents or files stored in or sent through XXORGANIZATION computer, dictation and/or voice mail systems are the property of the

XXORGANIZATION. To properly maintain and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. Since XXXORGANIZATION's computer and communication systems must be used for business purposes only, workers have no expectation of privacy associated with the information they store in or send through these systems.

3) At any time and without prior notice, XXORGANIZATION management reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on XXORGANIZATION computer, dictation and voice mail systems to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of XXORGANIZATION information systems.

4) To prevent accidental loss, all files and messages stored on XXORGANIZATION computer, dictation and voice mail systems are routinely copied to tape, disk, and other storage media. *This means that information stored on XXORGANIZATION systems — even if a user has specifically deleted it — is recoverable and may be examined at a later date by systems administrators and others designated by management as specified above*

5) XXORGANIZATION computer networks are private business systems, and not public forums, and as such do not provide First Amendment free speech guarantees. The XXORGANIZATION retains the right to remove from its information systems any material or information it views as offensive or potentially illegal.

6) Sexual, ethnic, and racial harassment — including unwanted telephone calls, electronic mail, and internal mail — is strictly prohibited and is cause for disciplinary action including termination.

7) When an employee leaves any position with XXORGANIZATION, files and documents may be reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. Employees should be aware that any files are subject to examination and deletion.

8) Unless the XXXDEPARTMENT has received instructions to the contrary, four weeks after any employee and/or consultant has permanently left the XXORGANIZATION, all files held in that user's personal folders will be purged.

COMPUTER SECURITY

Computer security is everyone's responsibility. Increasingly, our computer system stores information on our XXORGANIZATION as well as financial information that is necessary for the day-to-day operation of the XXORGANIZATION.

Our computer system's first line of defense – both internally and externally – is your password. It is the key to the cookie jar. Consequently, it is important that end-users not only protect their password, but be aware of and follow these requirements and conditions:

1) All user accounts are set with a "three strikes and you're out" rule. If you enter the incorrect password three consecutive times, the account is suspended and must be reset by the XXXDEPARTMENT.

2) Passwords expire 90 days from the last time the password was changed.

3) Passwords and user accounts provided to consultants and/or contract employees are set to automatically expire according to the terms of the contract.

4) All users are expected to know how to change or reset their password. The system will automatically notify you when your password is going to expire.

5) All passwords must have at least (6) characters, and should consist of a mixture of letters, numbers and symbols.

6) Passwords should not be any word that appears in the dictionary.

7) User passwords should contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation. Acceptable Characters are: A - Z, a-z, 0-9, and !@#$%&*()_-+=.

8) The initial passwords issued by the XXXDEPARTMENT should only be used during your first on-line session. At that time, you must choose another password before any other work can be done.

9) All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

10) Passwords should not be written down and left in a place where unauthorized persons might discover them.

11) Regardless of the circumstances, *passwords must never be shared or revealed to anyone* – unless requested or approved by the XXXDEPARTMENT.

12) Sharing your password exposes you to responsibility for actions that the other party takes with the password. If you need to share data, use electronic mail, shared folders on the LAN servers, and/or other mechanisms.

13) Staff should not leave their workstations unattended for an extended length of time without logging-out of the system and/or locking their workstation.

XXXDEPARTMENT staff should not attempt to test, or attempt to compromise internal computer security and access controls unless specifically approved in advance and in writing by the XXXPERSON of XXXDEPARTMENT.

All system privileges (rights) granted to users are evaluated on a periodic basis and are based upon need. User access rights may change.

APPROPRIATE USE POLICIES

General

Smoking, eating, or drinking while using a computer is strongly discouraged. Computers, printers, and other devices are sensitive and valuable equipment. Kicking or striking such equipment is prohibited.

XXORGANIZATION computer and communications systems must be used for business purposes. Incidental personal use is permissible only if the use:

(a) Does not consume more than a trivial amount of resources that could otherwise be used for XXORGANIZATION purposes;
(b) Does not interfere with productivity; and
(c) Does not preempt any XXORGANIZATION activity.

Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a personal luncheon.

Users of the XXORGANIZATION computing and communications systems must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by XXORGANIZATION management.

XXORGANIZATION information (databases, mailing lists, internal software, computer documentation, etc.) must only be used for purposes specifically allowed by management. Use of these information resources for any other reason will be permitted only after management has granted written permission.

XXORGANIZATION software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-XXORGANIZATION party for any purposes other than purposes expressly authorized by management.

The XXORGANIZATION requires strict adherence to software vendors' license agreements and copyright holders' notices. XXORGANIZATION staff may not make unauthorized copies of software.

Computer equipment provided by XXORGANIZATION must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior approval of the XXXDEPARTMENT. Furthermore, end-users should not install software, games, personal programs, screen savers, and/or any software purchased, received via email and/or downloaded from the Internet without the express permission of the XXXDEPARTMENT.

Computer Viruses

A computer virus is an unauthorized program that replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of virus infection include considerably slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers. Because viruses have become very complex, users must not attempt to eradicate them from their systems. If users suspect infection by a computer virus, they must immediately stop using the involved computer and call the XXXDEPARTMENT. Virus checking programs approved by the XXXDEPARTMENT are continuously enabled on all local area network (LAN) servers and networked personal computers (PCs).

Users may not place, download, load, or install any computer program on their workstations, laptop, network servers, or on computers connected to the network – regardless of the source -- unless this program has first been approved by XXXPERSON.

Appropriate Content of Communications

Telephones should always be answered cheerfully and courteously, by giving your department and name. Every effort should be made to assist the caller, including referral to the appropriate person if you cannot provide help as requested.

Professional conduct and appropriate content is required for all forms of communication. Faxes, telephones, and e-mail must all reflect appropriate content. Any misuse of these forms of communication will be a matter for discipline, up to and including dismissal.

Email

Our Email system consists of two parts – internal email and external email delivered and controlled by the Internet. Internally, the system is secure. All messages are stored in encrypted form that is inaccessible without your password.

Internet Email is not as secure. Unless the material is encrypted, staff should refrain from sending credit card numbers, passwords, and other sensitive data via electronic mail. XXORGANIZATION staff should adopt a "better safe than sorry" philosophy.

XXORGANIZATION staff should not use an electronic mail account assigned to another individual to either send or receive messages. If there is need to read other's mail (while they are away on vacation for instance), message forwarding, proxy access and/or other facilities must instead be used.

End users should be aware that the originator and recipient address of any and all email sent to an Internet address, or received from an Internet address, is tracked in a detailed audit log maintained by the XXXDEPARTMENT. As well, end-users should be aware that misaddressed messages are reviewed by IS staff for address correction or return to the originator.

The following general guidelines are offered as guidance in use of the Email system:

1) Use mailing lists wisely. We all receive several messages a day. Does your message really need to be sent to everyone in the group?

2) Post non-urgent items in the appropriate notice boards.

3) Utilize descriptive subjects that accurately describe the topic of the message.

4) Include a salutation ("Dear Bob" or just "Bob,") in every Email message. As messages are forwarded, copied or are sent outside of our internal system, the message header may change.

5) Sign your messages with your name. Again, as messages move through various systems, the message envelope you see may not be what the recipient sees.

6) The prohibition on outside programs mentioned previously includes any and all programs or other executable files received as email attachments. Only documents should be exchanged via email.

Internet

XXORGANIZATION management encourages XXORGANIZATION staff to explore the Internet for XXORGANIZATION -related business. Exploration for personal purposes must be done on personal, not XXORGANIZATION time. Likewise, news feeds, discussion groups, games, and other activities which are not related to an individuals job duties should be performed on personal time.

All users of the Internet should be aware that *our firewall creates a detailed audit log reflecting every request* for service, web site, downloaded file, etc., both in-bound and out-bound. Other safe "surfing" guidelines include:

1) Users should be careful about disclosing their real names, addresses, or telephone numbers on electronic bulletin boards, chat rooms, or other public forums reached by the Internet.

2) Staff should never send XXORGANIZATION credit card numbers, login passwords or other security information via the World Wide Web if it is in readable (un-encrypted) form. If you are unsure or unaware of the encryption status of a web site and/or how to check it, you should contact the XXXDEPARTMENT for assistance or utilize alternate methods. Most Internet sites feature an 800 number for orders.

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

4) It is relatively easy to spoof the identity of another user on public networks such as the Internet. Before staff releases any internal XXORGANIZATION information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed via digital signatures, but in cases where these are not yet available, other means such as third party references and telephone conversations may be used.

Telephone Usage (including Long Distance and Calling Cards)

The XXORGANIZATION telephone system and telephone services – including calling cards – must be used for business purposes only. Incidental personal use is permissible if the use:

1) Does not consume more than a trivial amount of resources that could otherwise be used for XXORGANIZATION purposes;
2) Does not interfere with productivity; and

3) Does not preempt any XXORGANIZATION activity.

Permissible incidental use of a calling card, for example, include reasonable calls home when traveling on business and staying overnight. Travel cards are provided to professional staff who must travel on a regular basis. These cards are issued and maintained by the XXXDEPARTMENT Department. Any loss or fraudulent use of these cards should be reported to the IS Manager immediately.

In order to reduce the risk of fraud, Travel Cards are periodically canceled and re-issued.

Users of the XXORGANIZATION telephone services must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by XXORGANIZATION management.

Voice Mail

In many cases, the first interaction the general public has with the XXORGANIZATION is our Voice Mail system. It answers the phone 24 hours a day, 7 days a week, 365 days a year. It is important that it reflect an appropriate level of professionalism and courtesy.

Voice Mail is provided as a supplemental tool for those who need to reach us. It is not intended to be the primary point of communication for individuals attempting to contact XXORGANIZATION staff. Every effort should be made to provide callers with an alternate person with whom to speak in your absence.

The following general guidelines are offered as guidance in use of the Voice Mail system:

1) Record both a personal greeting as well as an account name to identify the voice-mail box.

2) When recording the account name, use your full name. Do not use just your first name. The account name is used by the dial-by-name directory, hence should reflect your full name.

3) Keep your personal greeting current.

4) In your greeting, say how frequently you will be checking your messages. This gives callers some idea when you will be able to return the call. It also lets them know whether it's best for them to leave a message, try another extension, or press "0" to reach a live operator.

5) Make your greeting a friendly one. The tone you use in your personal greeting is as important as what it says. Callers will be more inclined to leave a message if your greeting sounds friendly, like an invitation to leave a message.

6) When leaving a message, speak naturally and smile. Believe it or not, smiling has a profound impact on the sound of your message. People will be more likely to return your call if you sound happy and upbeat.

7) Speak clearly. Whether recording a greeting or leaving a message, it's important to speak in clear, concise sentences. You will be more easily understood, and appear professional and organized.

8) Invite callers to dial "0". Use your personal greeting to remind callers they can press "0" to speak to a live person. This lets them know that once they have gotten into your mailbox they are not stuck with either leaving a message or hanging up.

9) In your greeting, ask your callers for the information you need, such as name, telephone number, the reason for calling and the best time to return their call. Don't waste time asking callers for the date and time of their calls because the system automatically time-stamps each message.

10) Check your messages regularly and return calls promptly. You can promote voice mail by answering messages from callers in a timely manner. Do not leave them wondering whether you got their messages; call them back. Even if you do not have an answer to their question or the information they need, call them back to let them know you got the message and are working on it.

11) Leave complete, detailed messages. Voice mail reduces telephone tag, but only if messages contain information other that just, "Hi, I called. Please call me back." Instead, include details that let the person know the reason for your call.

12) Use group broadcasting wisely. We all receive several messages a day. Does your message really need to be sent to everyone in the group?

13) Let repeat callers know how they can "skip" to the end of your personal greeting. Callers who just want to leave a message without listening to your entire greeting can skip to the tone by pressing the "*" on the keypad.

14) End the recordings of your greeting and account name appropriately – with the “1” key.

15) Don't slam down the telephone receiver when you're finished leaving a message. Everything you do will be recorded, including the sound of a loud hang-up or the other keys you press.

16) Verify your account name and greeting are recorded correctly by calling your own extension.

Other Telephone Issues

When using a telephone, staff should not use speaker phones, microphones, loud-speakers, tape recorders, or similar technologies unless they have first obtained the consent of both the originator(s) and recipient(s) of the call.

Copyright

Unless permission from the copyright owner(s) is first obtained, downloading and distributing copyrighted material over the Internet, or making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Laptops & Portables

A laptop and/or portable computer is a delicate piece of equipment. When traveling, staff should treat such equipment appropriately, and should not check computers in airline luggage systems. These computers should remain in the possession of the traveler as hand luggage.

A surge protector is provided with all laptops in use by staff. XXORGANIZATION staff must utilize this surge suppresser at home. Although recommended, this requirement is waived while using laptops and portable computers when traveling.

Laptops and other portable computer equipment remain the property of the XXORGANIZATION, and must be returned upon demand. Moreover, laptops and other portable computer equipment are subject to the same “appropriate use” guidelines and limitations as outlined above.