

# Company IT Policy

## General Policy

XXX (“Company”) is responsible for securing its computer systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy may result in disciplinary action in the form of temporary revocation of user access, regardless of the success or failure of the attempt. Permanent revocations can result from continued violations or from management decision.

The users of the Company computer systems are responsible for respecting and adhering to Company, local, state, federal and international laws. Any attempt to break those laws through the user of the Company computer systems may result in litigation against the offender by the proper authorities. If such an event should occur, the Company will fully comply with the authorities to provide any information necessary for the litigation process.

## 1.1 Privacy

All electronic equipment used by employees is to be considered property of the Company. All data, messages, or other files created while using the equipment is also considered property of the Company. The Company reserves the express right to monitor and review all activities of the employee, including information created or obtained by the employee.

This monitoring includes, but is not limited to, reviewing files or correspondence created by any software medium and periodic scans of an employee’s computer hard drive.

## **1.2 Personal Use of Computers**

Employees are not to place personal copies of software or data on any Company equipment. If an employee requires the software, the Company must purchase a copy. This includes, but is not limited to, games, screen savers, and questionable material. If found, the software or data will be removed and a memorandum sent to the XXX outlining what was found and the action taken to remove it.

It is Company policy that Company owned software is not to be taken home and installed on an employee's home computer for personal or Company use, regardless of the software's licensing agreement. The instances of abuse and the inability to monitor and control the software is beyond the scope of the Company.

## **1.3 Confidentiality**

Unless otherwise dictated by public disclosure laws, all information regarding the computers systems, or data created by employees, are to be considered confidential. Removing of data from the Company offices without the express consent of XXX is considered a breach of this confidentiality.

## **1.4 Violations of Company Policy**

Violations of this Company policy may lead to revocation of computer use or disciplinary action, including discharge.

## **1.5 Employee Signature**

All employees will be required to sign a Use of Company Network and Computers form (see Appendix) before access to the computer systems will be made available to the user. Refusal to sign the form will result in the employee not receiving computer system access and possible disciplinary action.

Once a user receives a network login account to be used to access the network and computer system, they are solely responsible for all actions taken while using that network login account.

## 2.1 Requesting A Network Login Account

When a new user needs network access, XXX must fill out the New User Request Form and sign it. The form needs to be returned to XXX along with the employee's signed Use of Computer and Network form for processing. Applying for a network login account under false pretenses is a punishable disciplinary offense.

## 2.2 Prohibited Actions

**Sharing passwords** - sharing your password with any other person is prohibited. In the result that you do share your password with another person, you will be solely responsible for the actions that other person appropriated.

**Use of Files** - deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.

**Changing Resources** - altering, or attempting to alter, yours or any other person's system configuration is prohibited. This includes attempting to gain greater access to the system or attempting to access data that you have not been given rights to.

**Use of System Resources** - improper use of system resources (e.g. waste of hard drive space, network bandwidth) can result, after the user is formally warned in writing, in either denial of further access to the system or further disciplinary action.

## Section 2 Use of Local and Wide Area Networks

**Use of Computer System** - use of facilities and/or services for commercial or personal purposes is prohibited.

**Unauthorized Use** - any unauthorized, deliberate action which damages or disrupts the computer system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

## 2.3 Appropriate Actions

All users should logout of the network and turn off computer equipment during nonworking hours (i.e. weeknights, weekends, vacations, holidays). This includes CPUs, monitors, printers and modems.

As a user of COMPANY X computer systems, you may be allowed access to other computer systems through the use of Company networks. This policy is used to describe types of security and prohibited actions regarding computer system security.

## 3.1 Computer Security Defined

**Physical Security** - this is the action taken to ensure that the computer system components (CPU, monitor, keyboard, mouse, modem, printer, etc.) are secure and not easily available by non-Company personnel. Physical security is the responsibility of the XXX.

**Access Security** - this is the action taken by the user to ensure that the computer system data is not compromised or made available to unauthorized personnel within and outside the Company. The use of passwords and file encryption are the most common.

## 3.2 Prohibited Actions

Accessing the use of computer systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited. The use of computer systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system or local system, is prohibited.

**Passwords** - decryption of system or user passwords, or any other method used in an attempt to gain unauthorized access to the computer systems, is prohibited.

**System Files** - the copying or transferring of system files is prohibited. The copying of copyrighted materials, such as third-party software is prohibited.

## Section 3 Security

**Unauthorized Use** - intentional attempts to "crash" network systems or programs is prohibited. Attempts to secure a higher level of privileges on any computer system are prohibited.

**Viruses** - the willful introduction of computer viruses or other disruptive/destructive programs into any Company computer system, or any external computer system, is prohibited. The unintentional introduction of a computer virus or other disruptive/destructive programs into any Company computer system, or any external computer system, by the failure to follow Company policy will result in disciplinary action.

This policy defines the framework for use of electronic message systems and communications media by employees of COMPANY X. This includes but is not limited to, electronic mail systems (e-mail), voice mail systems, calendar scheduling systems, faxes, Internet and other electronic media that generate, store, transmit and display correspondence for internal and external business communication purposes.

**4.1 Definitions Communications** is defined as a system for sending and receiving messages, as by mail and telephone.

Media is the plural of medium which is defined as a agent by which something is conveyed, accomplished, or transferred.

Communication media is that aspect of electronic messaging systems that contains the message.

**Employee** is a person who is a permanent employee, temporary employee, contractor, student intern or otherwise engaged at COMPANY X and has been given authorized access to any agency electronic messaging system.

**Encryption** is a method of "scrambling" data using cryptographic algorithm based on a secret key that is known only to the originating system and the destination system.

**Securing a device** means to log off the network, invoke a keyboard locking feature requiring a password, or otherwise make the device inaccessible.

## 4.2 Electronic Messaging Systems Expected Use

The Company will provide electronic messaging systems, making them available to COMPANY X employees as required subject to resources and other limitations. Employees with assigned access to electronic messaging systems are expected to use them.

### Section 4 Electronic Messaging Systems

Employees with access to electronic messaging systems are expected to check for messages on a frequent and regular basis and respond within a reasonable time as needed. An employee's use of Company-provided communications media is restricted.

Employees are expected to use Company provided communications media only for Company business. However, the Company recognizes the occasional need to exchange personal messages. These should be kept to a minimum, both in number and length. At no time should personal messages be sent in a way that charges the Company for transmission.


Employees shall not use Company provided communications media in a fashion that constitutes or involves any unlawful activity including but not limited to:

- A)** discrimination on the basis of race, creed, color, sex, age, national origin, marital status, religion, disability, sexual orientation or veteran's status
- B)** harassment, sexual and otherwise
- C)** copyright infringement
- D)** Expression of an employee's personal political beliefs or personal business interests.

Electronic communications resources are limited and employees must manage their allotted resources in a responsible manner. This includes but it not limited to deleting old messages and downloading e-mail messages to diskettes for long-term storage.

## 4.3 Confidentiality

Company-owned electronic messaging systems will provide data confidentiality and integrity. Employees must use reasonable means to minimize unauthorized access to electronic messages.



Employees are responsible for protecting messages from unauthorized access by maintaining password confidentiality and by securing the communications device to the extent possible before leaving it unattended.

Confidential and sensitive written information must be encrypted before transmitting electronically. This applies to information sent within the Company and especially information sent to external agencies.

#### **4.4 Electronic Messaging Privacy**

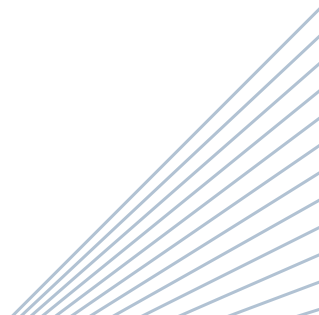
All Company information technology resources, including electronic messaging systems and files, are the property of COMPANY X. The Company may, under certain circumstances and in the course of normal business functions, access an employee's electronic messages without authorization from the employee.


#### **4.5 Sending of Electronic Messages Globally**

Electronic messages sent globally (i.e., to “\*ALL”) must be appropriate for type and content. Examples of appropriate global messages are those that pertain to normal operations of the Company such as training and security alerts.

#### **4.6 Electronic Messaging Retention**

Electronic messages conform to all applicable statutes and regulations governing public records, records retention and public disclosure. E-mail messages can only be stored for a limited time on the system. If an e-mail message needs to be preserved, it should be moved into another media for storage. Information requiring longer retention should be printed and stored as hard copies.





The Internet, when used appropriately, is an extremely valuable tool for COMPANY X staff. It offers direct access to numerous agencies and organizations whose publication and information are sought by staff on a daily basis. Its use enables staff to locate materials without leaving their workstation. In addition, more elusive information can often be located in a highly time efficient manner by subject searching on the Internet or querying a list server. It benefits COMPANY X to provide direct access to the Internet to employees; contractors and volunteers who can use it to better perform their jobs.

**5.1 Definitions Internet** - worldwide network of networks and computers.

**Hacking** - attempting to break into another system on which you have no account, and is treated as malicious intent.

**Netiquette** - a word made from combining “Network Etiquette” which is the practice of good manners in a network environment.


Flame wars - angry e-mail exchanges.

**Surfing** - random Internet browsing, normally not work related.

## **5.2 Guidelines**

When accessing the Internet, employees are representing COMPANY X, therefore all rules of conduct and law that apply in your regular workplace also apply on the Internet.

COMPANY X has the right to review user accounts, workstations and file server space in order to make determinations on whether specific uses of the information systems are appropriate. COMPANY X may revoke an employee’s, contractors or volunteer’s access to the network and network services when there has been a clear violation of acceptable.





## **Section 5 Internet Access**

use principles and guidelines. In addition, where violations occur, employees, contractors and volunteers are subject to any disciplinary or corrective actions or penalties proscribed in law, rule or policy.

### **5.3 Acceptable Uses of the Internet**

COMPANY X encourages appropriate use of on-line resources. Acceptable uses include, but are not limited to:

XXX  
XXX  
XXX

the facilitating communication with other agencies or business partners, facilitating discussions aimed at professional development, gathering information on industry trends, use in grant related activities, legal and policy research, gaining timely access to government publications and statistics, and generally advancing the information needs of the organization.

### **Prohibited Uses of the Internet**

Inappropriate behavior may result in disciplinary actions ranging from verbal warnings to termination of network services and/or employment with COMPANY X. The severity of the misbehavior governs the severity of the disciplinary action. Inappropriate on-line behavior in the workplace would include, but is not limited to:

XXX  
XXX  
XXX

unauthorized attempts to break into any computer whether of **COMPANY X** or another organization (Hacking), using Company time, equipment and/or other resources for non-work-related activity, personal gain or recreation, sending threatening messages, sending racially and/or sexually harassing messages, theft, or copying, of electronic files without permission, sending or posting **COMPANY X** confidential materials outside the Company, or posting **COMPANY X** confidential materials inside the Company to non-authorized personnel, sending chain letters through electronic mail, “surfing” pornographic and sexually oriented sites, random “surfing” and “flame wars”.

### **Internet Access Authorization**

Access to the Internet will be provided to **COMPANY X** employees, contractors and volunteers when deemed appropriate for their work. This is at the discretion of **XXX** or an elected department head subject to resources and other limitations.

### **COMPANY X Use of Computer and Network Form**

I hereby consent that COMPANY X, or its authorized representatives, may monitor, review, and/or copy any information on the electronic data processing system, including the electronic mail system, whether stored or in transit, at any time, and may, without further notice, disclose such information to any third party or parties, including government and law enforcement agencies.

### **Prevention of Unauthorized Access**

I will maintain the confidentiality of my system password and will not permit access to my network account or to my electronic mail account by any person unless my immediate supervisor has approved such access in advance. If my password is disclosed to any other individual, for whatever reason, or if to my knowledge the security of my account is otherwise breached, I will immediately notify XXX or my immediate supervisor at the time.



Acknowledgement of COMPANY X Computer Usage Policy and Procedures

This is to acknowledge that I have read and understand COMPANY X Computer and Network Policies and Procedures. I understand that failure to follow the provisions of the Policies and Procedures could lead to the loss of my computer system privileges and/or more severe disciplinary action.

By signing below, I agree to abide by the Company policy.

Employee Name (Please Print): \_\_\_\_\_

Department: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

