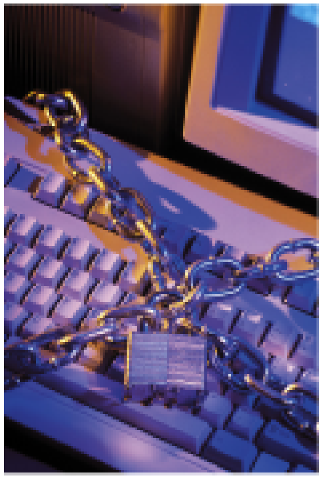
Cyber Security

Internet and Acceptable Use Policy Template

A Non-Technical Guide

Essential for
Business Managers
Office Managers
Operations Managers



Multi-State Information
Sharing and Analysis Center
(MS-ISAC)

This appendix is a supplement to the *Cyber Security: Getting Started Guide,* a non-technical reference essential business managers, office managers and operations managers. This appendix is one of many which is being produced in conjunction with the *Guide* to help those in small business and agencies to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.msisac.org

Acknowledgement

Special thank you to Rochelle Stein and the Town of LeRoy, NY for their contribution to this paper.

Photos By: © 2008 Jupiterimages Corporation

Glossary

Encryption –The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Locally Managed Network – Safeguards in place:

- On a secure server
- Restrict administrator rights

Restricted Information – pertains to information which is not public information, but can be disclosed to or used by organization representatives to carry out their duties, so long as there is no legal bar to disclosure.

INTRODUCTION

[Insert your organization here] Acceptable Use Policy specifies policy for the use of information resources and information technology systems. Enforcement of this acceptable use policy is consistent with the policies and procedures of this organization.

Being informed is a shared responsibility for all users of [Insert your organization here] information systems. Being informed means, for example:

- Knowing these acceptable use policies and other related rules and policies,
- Knowing how to protect your data and data that you are responsible for,
- Knowing how to use shared resources without damaging them,
- Knowing how to keep current with software updates,
- Knowing how to report a virus warning, a hoax, or other suspicious activity, and
- Participating in training.

POLICY

Compliance with this policy is mandatory for all officials, employees and contractors of this organization. This policy applies to all [insert your organization here] information, computer systems and data that is used for official [insert your organization here] business regardless of its location.

1. Authorized Use

Users must not use other users' passwords, userids, or accounts, or attempt to capture or guess other users' passwords. Users are also restricted from using business equipment for personal use, without authorization from your [insert your organization here]. Users must not hide their identity for malicious purposes or assume the identity of another user.

2. Privacy

User files may be subject to access by authorized employees of [insert your organization here] during the course of official business. Accordingly, users should have no expectation of privacy and their activity may be monitored.

3. Restricted Access

Users must not attempt to access restricted files or portions of operating systems, security systems, or administrative systems to which they have not been given authorization. Accordingly, users must not access without authorization: electronic mail, data, or programs, or information protected under state and federal laws. Users must not release another person's *restricted information*.

4. Proper Use of Resources

Users should recognize that computing resources are limited and user activities may have an impact on the entire network. They must not:

- misuse email — spread email widely (chain letter) and without good purpose ("spamming") or flood an individual, group, or system with numerous or large email messages ("bombing"), or
- use streaming audio, video or real time applications such as: stock ticker, weather monitoring or Internet radio.

5. Protecting Information and Shared Resources

Users must:

- Follow established procedures for protecting files, including managing passwords, using *encryption* technology, and storing back-up copies of files.
- Protect the physical and electronic integrity of equipment, networks, software, and accounts on any equipment that is used for [insert your organization here] business in any location.
- Not visit non-business related websites
- Not open email from unknown senders or email that seems suspicious.

- Not knowingly introducing worms or viruses or other malicious code into the system nor disable protective measures ie: antivirus, spyware firewalls.
- Not install unauthorized software.
- Not send restricted or confidential data over the Internet or off your *locally managed network* unless appropriately encrypted.
- Not connect unauthorized equipment or media, which includes but is not limited to: laptops, thumb drives, removable drives, wireless access points, pdas, and mp3 players.

6. Civility

Users must not harass other users using computer resources, or make repeated unwelcome contacts with other users. Users must not display material that is inappropriate in an office environment for example, consistent with [insert your organization here] policies.

7. Applicable Laws

Users must obey local, state, and federal laws including laws on copyright and other intellectual property laws.