

Creating Your Acceptable Use Policy

By Robert H. Spencer, Ph.D.

The best way to truly protect the best interest of your company is to place the proper written policies in place. While there is no single “correct” policy statement, I have researched a number of examples and compiled a sample that seems to cover the territory. As always, this is only a sample, and I suggest you seek advice of counsel before implementing your own version.

The acceptable use policy defines the acceptable use of automated data processing equipment, software and communications as provided by your company. Everyone in the company must be expected to follow the written policy without exception. The policy should be both in writing and perhaps placed on the company Intranet for easy access.

So, what defines an Acceptable Use Policy? To provide guidance as to what to place in your policy statement, let’s define a few unauthorized uses for a computer account.

Users will not violate copyright laws and their fair use provisions through inappropriate reproduction and/or distribution of music (MP3, etc.), movies, computer software, copyrighted text, images, etc.

Users shall not use company computers or network facilities to gain unauthorized access to any computer systems. Using programs intended to gain access to unauthorized systems for any reason or purpose is strictly prohibited.

Users shall not connect unauthorized equipment to the company’s network, to include hubs, routers, printers or other equipment connected to the company’s network directly or via remote attachment.

Users shall not make unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

Users will not associate unapproved domain name sites with a company owned IP address.

Users will not knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.

Users will not knowingly or carelessly run or install on any computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer system or network. This

includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.

Users will refrain from activity that wastes or overloads computing resources. This includes printing too many copies of a document or using excessive bandwidth on the network.

Users will not violate terms of applicable software licensing agreements or copyright laws.

Users will not use company resources for commercial activity, such as creating products or services for sale.

Users will not use electronic mail to harass or threaten others, or to send materials that might be deemed inappropriate, derogatory, prejudicial, or offensive. This includes sending repeated, unwanted e-mail to another user.

Users will not use electronic mail on company-owned, or company-sponsored, or company-provided hardware or services to transmit any information, text, or images that would be deemed offensive, inappropriate, derogatory, prejudicial, or offensive.

Users will not initiate, propagate or perpetuate electronic chain letters.

Users will not send inappropriate mass mailings not directly associated with, or in the performance of, the routine course of duties or assignments. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

Users will not forge the identity of a user or machine in an electronic communication.

Users will not transmit or reproduce materials that are slanderous or defamatory in nature, or that otherwise violate existing laws, regulations, policies, or which are considered to generally be inappropriate in a work place.

Users will not display images or text that could be considered obscene, lewd, or sexually explicit or harassing in a public computer facility or location that can be in view of others.

Users will not attempt to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

The list above defines each of the specific areas of concern a company usually encounters. The following takes these concerns and places them in an appropriate text for a policy statement. Again, you should review your policies carefully, have them reviewed by legal counsel for wording and enforceability appropriate to your geographic area.

Acceptable Use Policy for Sample Company

Sample Company encourages the sharing of information, comprehensive access to local and national facilities to create and disseminate information, and free expression of ideas. General access facilities and infrastructure are provided to further these purposes. There is an obligation on the part of those using these facilities and services to respect the intellectual and access rights of others--locally, nationally and internationally.

Computing resources and facilities of Sample Company are the property of the company and shall be used for legitimate activity related to the performance of the duties and responsibilities of the users only, administrative, public service, or approved contract purposes. Supervisors may, at their discretion, allow personal use by the employee of these resources that does not interfere with the institution or with the employee's ability to carry out company business. Individuals who disregard elements of this policy will be subject to appropriate disciplinary and/or legal action by Sample Company. Use of company computing facilities for personal or commercial use is not authorized. Use of company computing facilities for educational purposes must be consistent with other training educational programs. The use of company computing facilities for higher education degree seeking or certification programs may only be done with the specific written approval of the appropriate supervisor.

Individuals and non-company organizations using the company's facilities to gain access to non-company facilities must be cognizant of and observe the acceptable use policies of the company at all times.

Failure to observe these policies will result in immediate disconnection or loss of use privileges, as well as possible disciplinary action or termination at the discretion of the offending party's supervisor or department head based on the nature and severity of the offense.

Unauthorized viewing or use of another person's computer files, programs, or data is prohibited. All users should also be aware that all programs and all files are deemed to be the property of the company, unless the individual has a written agreement signed by an appropriate representative or officer of the company. Federal or state law may require disclosure of individual computer files

which are deemed public records under the state public records statute and that state and federal law may prohibit the disclosure of certain records as well.

Entry into a system, including the network system, by individuals not specifically authorized (by group or personally), or attempts to circumvent the protective mechanisms of any system, are prohibited. Deliberate attempts to degrade system performance or capability, or attempts to damage systems, software or intellectual property of others are prohibited.

The electronic mail system shall not be used for "broadcasting" of unsolicited mail or for sending chain letters, and the communication system shall not be used for sending of material that reasonably would be considered obscene, offensive, or threatening by the recipient or another viewer of the material.

The company reserves the right to monitor and record the usage of all facilities and equipment, and all software which is the property of the company by ownership, lease, rent, sponsorship or subsidy, if it has reason to believe that activities are taking place that are contrary to this policy or state or federal law or regulation, and as necessary to evaluate and maintain system efficiency. The company has the right to use information gained in this way in disciplinary or criminal proceedings.

The Federal Copyright Act nearly always protects commercial software. Use of company facilities or equipment for the purpose of copying computer software that does not contain specific permission to copy (some licenses do allow the making of one copy for backup) is prohibited. The unauthorized publishing of copyrighted material on a company server is prohibited, and users are responsible for the consequences of such unauthorized use.

An individual's access to computer resources may be suspended immediately upon the discovery of a violation of this policy.

This policy contains the company's complete acceptable use policy and replaces any pre-existing policy issued before *Month Day, Year*. For questions about this policy, contact *Name and Contact Information Here*.

Failure to comply with any of the above policies may result in termination of your Sample Company network services, disciplinary action, and/or criminal prosecution. The company reserves the right to terminate any company network connection without notice if it is determined that any of the above policies are being violated.