PROBLEMS ADDRESSED
Because more companies are now using the Internet as a means of communication and research, IS executives are writing and implementing an acceptable usage policy for corporate use of the Internet. Such a document may be called an Internet use policy, the networking portion of the computer use policy, or the Internet addition to the personnel manual. The goal of this policy is to list the rules and standards for employees using computers, networks, and, particularly, the Internet. Although the acceptable use policy can be incorporated into other existing documents, it is generally provides more company protection if it is a separate document.

Why is the acceptable use policy so important today? Legal liability for Internet actions can quickly shift from the employee to the employer. If management allows access to inappropriate Internet sites without either warning users or blocking access, management can become liable, along with the employee performing illegal actions.

WRITING AN ACCEPTABLE USE POLICY
IS managers, or a department employee, must write the acceptable use policy. It is better to have the fewest number of people — preferably one person — writing the acceptable use policy. Although this suggestion may conflict with many corporate cultures, the acceptable

PAYOFF IDEA
The job of an acceptable use policy is to explain acceptable Internet and computer use within an organization and to protect both employees and the organization from illegal acts. This article describes such policies: what they should cover and how they are most effectively activated.
use policy is different than a product manual or marketing white paper. The acceptable use policy is a legal document that binds the behavior of employees within certain boundaries.

With fewer authors the number of viewpoints within the acceptable use policy is limited. Your employees must be clear about the purpose of the acceptable use policy, their Internet and computer use responsibilities, and the penalties for misuse of company resources, including time. More authors, or up-the-line editorial changes, will muddy the acceptable use policy. Internal contradictions within the acceptable use policy will leave loopholes for employee lawyers to exploit.

After the policy is written, a committee that oversees employee compliance with the terms of the agreement should meet and approve the acceptable use policy before distributing the document. This is the time for any comments, suggestions, additions, or deletions. While the committee is welcome to offer changes, only the author should implement them. Again, the consistency of viewpoint is important.

Legal review comes after the committee has approved the acceptable use policy. Here a philosophical decision must be made. Often, lawyers want long, complicated documents that spell out every possible infraction and associated punishment, while business managers want short documents that can be interpreted in the company’s favor. The length and level of detail should reflect the corporate culture and views of upper management.

The document should be a part of the employee handbook. In some states, these handbooks are regarded as a legal contract. Corporate counsel will be able to answer that question for the states where the company operates.

Be aware that the longer the policy, fewer number of employees will read it to the end. In most states, employees are bound by the conditions of the policy. However, holding employees liable for a document they have not read will be seen as a cold, heartless corporate maneuver. Employees who feel betrayed contact lawyers far more often than those who feel they were treated fairly. Although it is legal in some states for companies to ignore the promises they make in employee handbooks, the antagonism employees may feel as a result of them guarantees lawsuits.

POLICY SCOPE AND OVERVIEW

Does your company already have computer-use policies? How about company telephone, fax, and mail use? Is there a security policy in place? Some companies, remiss in providing policies in the past, try to incorporate all these into the acceptable use policy. Although this is legal, it is confusing to employees. The acceptable use policy will be more valuable if targeted strictly to Internet and other computer networking concerns.
E-Mail

Because E-mail is the most popular Internet application, control over its use is important. The good part of E-mail is that an appropriate analogy can be made to traditional mail.

One company includes this statement: “Remember that E-mail sent from the company travels on the company’s electronic stationary. Your E-mail appears to the recipient as if it were sent on company letterhead.”

Your security policy, if separate, should cover information about E-mail accounts, such as forging identities. Instructions concerning appropriate E-mail use can also be included in the acceptable use policy.

Other E-mail guidelines that some schools and companies prohibit:

- Sending harassing, obscene or other threatening E-mail
- Sending junk mail, for-profit messages, or chain letters
- Sending or receiving sexually oriented messages or images
- Transmittal of confidential company information
- Divulging employee medical, personal, or financial information
- Personal messages

Also often included is a request that reasonable precautionary means be taken against importation of computer viruses.

Employees may also be reminded of the importance E-mail is to communications within a company. Whether an employee must be told when the company monitors communications is advisable according to some lawyers, but not others. Either way, if every employee signs the acceptable use policy accepting E-mail monitoring on a random basis, they may pay more attention to the following the rules.

Employees should have no expectation that E-mail messages are private and protected by a privacy law. Make sure each user understands that some messages will be read by management, even if messages are only spot-checked.

Do not keep E-mail message for longer than 90 days. Lawyers are now routinely demanding E-mail archives during lawsuit discovery. If your company is sued for any reason, the opposing lawyers will try to read all internal and external E-mail messages for the time in question. No E-mail archives means no embarrassing quotes and off-the-cuff remarks that will cost you in court. Some large companies refuse to back up E-mail files for this reason.

World Wide Web Resources and Newsgroups

The Web is often criticized as a giant productivity sink hole. Corporate managers rank employee time wasted on the Internet as their number two concern right behind security. Management often wonders how many
employees are frittering away hours on company time perusing the Web on company equipment.

While newsgroups full of equivalent professionals in other companies provide great benefit to your company employees, the nontechnical press focuses on the “alt.sex.*” hierarchy of newsgroups. Someone in your management will be determined to limit access to all newsgroups, just to keep the alt.sex. groups out of the company.

Newsgroups are where the majority of defamation happens; “flame wars,” are when people become angry and make unprofessional statements, which result in legal action against the employee and the company represented by the employee. Often, other readers of the newsgroup will send copies of messages to the postmasters of the flame war participants. Management should counsel employees accused of involvement and if this does not work, unplug them from the newsgroup access list. No sense risking a lawsuit when there may be a good chance of statements being made that have no positive value to the company.

Be upfront with management about the existence of inappropriate Web servers and newsgroups. But also note that some Web servers and newsgroups are valuable. Also be sure to mention that each user can be monitored and the name, date, time online, and amount of material downloaded from any inappropriate network source can be obtained.

This will allow the actions of each and every corporate user during each and every network communication to be logged. If the proper firewall or proxy server to monitor users is not in place, make this a priority.

Realize that some time will be wasted on the Web, just as time is wasted reading through trade magazines looking for articles that apply to your company. Every profession has trade magazines that offer articles and information in exchange for presenting advertising to the reader. The Web, to some people, is becoming nothing more than a huge trade magazine, offering helpful information interspersed with advertising. Some employees research information more than others and will use their Web client more. Know which employees should be using the Web.

Web guidelines may be mentioned in the acceptable use policy. Sample restrictions may include:

- Viewing, downloading, displaying, or distributing obscene images
- During work hours Web browsing should focus on business-related searching

Remind your employees regularly that obscenity in the workplace will not be allowed. Modify the second bullet point to match the company’s comfort level regarding employee use of the Web.

Other restrictions may include:

- Downloading or uploading of nonbusiness images or files
• E-mailing of harassing, obscene and/or other threatening messages
• E-mailing of junk posts or “for-profit” messages
• Posting of articles to groups unrelated to the article’s subject matter
• Posting of company advertisements in any newsgroup
• Posting of messages without an employee’s real name
• Copying of newsgroup information to any other forum

Several acceptable use policies address defamation obliquely. Some examples of the language included in those policies include statements restricting “comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs” or “send[ing]/receiv[ing] messages that are racist, inflammatory, sexist, or contain obscenities”

Whether these are politically correct or good business sense depends on the individual company. These same courtesy restrictions apply to E-mail, but E-mail lacks that extra edge brought when thousands of readers see your company name attached to the ranting of one overwrought employee.

IRC (Internet Relay Chat) and MUDs (Multi-User Domain) have not been mentioned because they have no redeeming professional use. Employee use should be tolerated.

In case employees are confused about the company’s rights to monitor employee computer use, include a line such as: “All computer communications are logged and randomly reviewed to verify appropriate use.”

The term “appropriate use” is carefully chosen. If the acceptable use policy says the words “dirty pictures” or “indecent,” employees (and their lawyers) can argue that “dirty” and “indecent” is in the eye of the beholder: Inappropriate covers more activities than any other term. Another option is obscene, which is a legal term that applies just as well to computers as to magazines, books, and videos.

Penalty for misuse should range up to and include termination. If an employee must be terminated, do so for work-related causes, rather than Internet causes. Free speech advocates can get involved when an employee is fired for inappropriate use of the Internet, but not when an employee is terminated for wasting too much time on the job and disobeying orders.

Netiquette Addendum
Some companies spell out appropriate E-mail, newsgroup, and Web communication guidelines within their acceptable use policy. This is a noble endeavor, but slightly misguided. Company guidelines on Internet communications are likely to change more often than your restrictions on inappropriate Internet use and discipline for infractions.

Because an acceptable use policy should be signed by each employee, any changes to netiquette embedded in the acceptable use policy will
require a new signature. The logistics of this process can quickly become overwhelming.

Put the rules of Internet behavior in a separate addendum. Changes to E-mail rules, for instance, will not negate the acceptable use policy, nor will a new signature be necessary.

ACTIVATING THE POLICY

Getting employees to sign an acceptable use policy can be tricky. Small-to medium-sized companies can handle the logistics of gathering signed copies of the acceptable use policy, although there will still be considerable time expended on that effort. Large companies may find it impossible to ship paper policies all over the world for signatures and get them signed, no matter how much time and effort they devote.

The best case is to get a signed acceptable use policy from each employee before that person is connected to the Internet. Training classes offer an excellent chance to gather signatures. If software must be installed on client computers, the policy should be presented, explained, and signed during software loading.

Unfortunately, many companies already have granted Internet access before developing an acceptable use policy. This is not the wisest course, but is common. Other companies do not offer training or cannot gather signed copies.

It is important to send copies of the policy to each employee with Internet access. Copies should also be posted in public places, such as break rooms and department bulletin boards. The policy should also be added to the existing personnel manual or employee handbook. An E-mail should also be sent to users every quarter reminding them of the acceptable use policy and where they can read a copy. These efforts should stop any employee contentions concerning Internet restrictions.

THE ACCEPTABLE USE POLICY COMMITTEE

An Acceptable Use Policy Committee should be formed from employees from each department. Each member should be notified in advance of the first meeting and have adequate and timely background information on the task of the committee.

The following list contains the requisite committee positions and their expected contribution:

- Computer systems manager. Provides technical details of Internet access and monitoring.
- Company lawyer or human resources official. Provides legal aspects of workplace rules.
- Executive management representative. Guarantees your committee will not be ignored.
• Union representative. Has knowledge of laws for union employees.
• Employee representative. Represents employee concerns and interests.

This committee will discuss all Internet concerns, and should probably meet every two weeks. Once the Internet connection is old news, once a month may be enough. The interval is dictated by the number of security incidents and employee discipline actions to be resolved.

In extreme cases, such as an employee action that could result in company liability or criminal prosecution for someone, the committee must meet immediately. The grievance policy in cases of Internet abuse should be clear and well known to all employees. It also is important that employees know who is on the committee. Secret committees are repressive, but open committees can encourage good will within the company. Strongly consider setting up an internal E-mail address for your committee, and use it for questions and as an electronic suggestion box.

The most effective deterrent to misdeed is not the severity of discipline but the inevitability of discovery. Remember, the goal is to make the Internet serve the company, not to find excuses to discipline or fire employees. At the first committee meeting, the following questions should be answered:

• Will employees be fired for Internet misuse?
• What is the penalty for the first offense? The third? The fifth?
• Will the police be called for stolen software or obviously obscene images?
• Should other employee policies be modified to support the Internet connection?
• Are any insurance policies in place to protect against hackers or employee misdeed? Should some be added?
• How often will employees be reminded of company Internet guidelines? How will this be done?

Discipline is particularly tough. After all, if an employee is wasting hours per day on the Internet, the department manager also should be disciplined for improper management. Waste of time on the Internet is not a technology issue, but a management issue.

Outsiders with an executive mandate to punish miscreants are never popular and often are sabotaged by the very employees they oversee. Keep department managers in the loop as long as possible. Exceptions include security violations and illegal acts: department managers must be informed in these instances, but company security or local police will handle the situation.
RECOMMENDED COURSE OF ACTION

The job of the acceptable use policy is to outline acceptable Internet and/or computer use and behavior. The committee dedicated to enforcing the provisions of the policy must publicize the policy and monitor employee compliance. Infractions must be handled quickly, or employees will assume the Acceptable Use Policy is not important, and compliance levels will shrink. Proactive Internet management will drastically lower the chances of Internet-related lawsuits, arguments, and misunderstandings.

James E. Gaskin is an author and consultant specializing in technical subjects and technical policy issues, such as corporate politics and the Internet. He can be reached at james@gaskin.com.