Developing an Internet Access Policy

A Guide To Developing Your Company's Internet Access Policy (IAP)

www.SurfControl.com

Notices

This document serves as a guide for general information only. It does not include nor should it be considered as legal advice. You should seek advice from your legal counsel to assist you in establishing an appropriate Internet Access Policy.

SurfControl plc
100 Enterprise Way, Suite A110
Scotts Valley CA 95066
800 368 3366 or 831 431 1300

Table of Contents

Welcome to Cyberspace

For many businesses these days, the Internet is indeed the New Frontier. But as companies rush headlong onto the World Wide Web to stake a claim in this exciting new digital territory, they're finding that for all its promise, the unbounded Internet environment can be a pretty tough place.

Issue 1: Employee Productivity

Although it is arguably the most important information and communication resource in human history, the Internet is a seductive place. From vital online market information to last night's sports scores, online games and day trading, a chat room or IRC, you can get almost anywhere in one click. How many hours of lost productivity can your company afford?

Issue 2: Network Bandwidth

Combine recreational surfing with bandwidth-intensive activities such as streaming audio and video, MP3 downloads, and image downloads and you have a significant impact on network performance that impedes business traffic.

Issue 3: Legal Liabilities

Letting employees surf anywhere on the Internet can lead them to stray to clearly inappropriate sites— sexually explicit sites and those promoting violence, hate speech, and gambling. This kind of surfing can lead to lawsuits, harassment charges, and even criminal prosecution. Protect your employees and your company by promoting intelligent Internet use.

Does all this mean that your company ought to stay off the Internet? Of course not. But you should be alert to some of the pitfalls amid all the business potential of the Internet. The good news is that most, if not all, of these pitfalls can be avoided by developing and implementing an effective corporate Internet Access Policy (IAP), and using proven filtering software to assist your efforts.

Why Your Company Needs an Internet Access Policy?

When it comes to the Internet, consider the risk of being without one. The Internet can be a powerful and versatile business asset. It can be used to improve communications with customers and partners, reduce internal cycle times, disseminate information internally and externally, and build new client relationships. Certainly, it provides, at little cost per user, a vast and highly customizable information resource.

But how much of a good thing is too much? You wouldn't want employees browsing the public library for hours every day, for example, or using business phone lines for unlimited personal calls to Sri Lanka. So why would you want them building up their online music collection, planning their next vacation, or ordering their holiday gifts online on company time?

Sooner or later, you'll have to institute an Internet Access Policy that explicitly lets users know what is and what is not allowed. In view of the fact that failure to properly manage Internet access can expose your company to serious legal liability—not to mention the significant "fritter-factor" drain on bottom line productivity—sooner is definitely better.

Make It a Team Effort

Developing corporate access guidelines should be a team effort. According to Gartner Group, "The separation of creation and implementation of the policy is a recipe for disaster." (*Strategic Analysis Report 9/23/96, Gartner Group*).

Setting corporate limits on Internet use can be an emotionally charged subject, linked as it is to issues of personal privacy and individual responsibility. For that reason, it's prudent to avoid any hint of "top-down" policy-making. Rather, it will be better if both the articulation of the business need for an IAP and the IAP itself are developed by representatives of every aspect of the business: senior management, information technology, business unit managers, human resource, legal and interested user groups.

The goal should be not only to clarify the company's policy regarding use of the Internet to shield the enterprise against potential liability, but also to encourage effective use of the resources, and to provide positive direction for their appropriate use.

Building the IAP

Developing an Internet Access Policy has a valuable side benefit for most organizations. It provides an ideal forum for crystallizing the company's goals and expectations for the Internet. And that's a good place to start, with a clear statement of the valid business reasons for providing an Internet connection.

Keep in mind that Internet access needn't be "all or nothing." You can restrict certain services, type of access, time of day, and length of connection exactly as you can for internal network connections. It helps to think of Internet access as a privilege, rather than an inalienable right (although some users are sure to argue otherwise). Here are some of the areas to consider when building an IAP:

Don't let the Internet drive your company to distraction.

There's no denying it. The Internet is the biggest potential time-waster since the water cooler. ("Just a couple of minutes to relax, and I'll be right back to work...")

Your policy should be explicit about the level of personal surfing that is acceptable. Some organizations—especially those whose business places a premium on creativity—might even encourage employees to roam cyberspace as part of their jobs. Some may choose to limit Internet activity to strictly work-related sites and activities. Others may look for the "happy medium."

What about off-hours activity?

Depending on the type- and cost- of your physical connection, you may decide to allow, and even encourage, appropriate personal use of Internet resources during non-work hours. And you may or may not choose to place restrictions on the content, types of sites visited and specific activities.

But remember, even during off-hours, the sites your employees visit reflect directly on your company's image. (And any well-equipped Webmaster can determine with a reasonably high degree of accuracy where traffic is coming from.) Nor does off-hours usage lessen the company's legal responsibility regarding sexual harassment, misrepresentation and other issues.

Covering your assets.

Every employee using Internet resources should have a clear understanding of the legal issues involved. These include:

- **Sexual harassment** as a result of bringing objectionable or sexually explicit material into the workplace. Although this legal territory is still somewhat uncharted, if an employee downloads objectionable materials - pornography, for example - and another employee sees it, your company could be liable. Even worse, if a user downloads materials that are illegal within your community, your company might even face criminal charges.
- **Copyright infringement** can happen unintentionally. An employee downloads a software program, a photograph or a proprietary document in all innocence, thinking that, because it's available on the Internet, it's "free." It's not.

- **Misrepresentation** can also occur unintentionally, too, particularly through the use of email. Employees should know, and should make it clear to the people with whom they communicate, that opinions expressed via email and other electronic media are their own, not the company's.

Meet your new cyber-ambassadors.

With Internet access, many employees who previously had no occasion to interact with customers or business partners may now become active communicators. What's worse than receiving a garbled, misspelled, incoherent email message? Realizing that one of your staff sent it.

Some things are better not shared.

Now that it's possible to send an email to millions of people with the touch of an enter key, you'll want to remind employees at all levels about the importance of protecting valuable company information. Business plans, marketing strategies, sales results, economic projections - any and all of these can be sent literally anywhere with a keystroke. Obviously, some things simply shouldn't be shared. And without encryption, employees have to realize that nothing on the public network is private.

Make network security part of everybody's job description.

Your Internet link to the wide world is also the wide world's link to your company. Certainly, you have enterprise security measures in place, but even the most secure firewall can be compromised by an employee's accidental disclosure of a password, or - to a determined hacker - even an IP address. The sad truth is that far more security problems are caused by carelessness and inattention than by malicious hacking.

Also keep in mind that even the best-intentioned employee can inadvertently bring a network down with a virus retrieved from "off the Internet." If you plan to use any type of virus scanning software—and you should!—your users should know that their email and outside connections would be scanned as a normal part of network security.

Don't believe everything you read - especially on the Internet!

All information received or retrieved via the Internet should require authentication and validation before it is relayed or used for business purposes. Enough said.

What Should Be In Your IAP?

Now that you have decided to develop an IAP for your company, this information, along with a series of tips, will guide you in the successful development and implementation of such a policy.

General Principles

Lay out the general principles guiding the development of this policy. This section should help your organization to understand the reasoning behind the IAP and get philosophically aligned with it. Explain to your employees why you feel that a policy for acceptable use of the Internet is advisable within your company. Here's an example:

> *Use of the Internet by Company employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the Company and its business units. The Internet is to be used in a manner that is consistent with the Company's standards of business conduct and as part of the normal execution of an employee's job responsibilities.*

Company-provided Internet/Intranet and email privileges, like computer systems and networks, are considered company resources and are intended to be used for business purposes only. Employees should be aware that usage is monitored for unusual activity.

Conditions of Use – The Heart of your IAP

First and foremost, the policy includes "do's and don'ts" of Internet use within the organization. Be sure to clearly define which practices are considered unacceptable, and may be subject to disciplinary action, including written warnings, revocation of access privileges, and, in extreme cases, termination of employment. Also let your organization know that the Company reserves the right to report any illegal activities to the appropriate authorities.

In addition, there are several types of Internet-related activities and behavior that you may wish to call out specifically, and note that they may result in some kind of disciplinary action. Here are some examples of the types of things that are typically included:

Proper Corporate Representation

Make it clear whether or not corporate email accounts, Internet IDs and Web pages may be used for anything other than corporate-sanctioned communications. If personal email is permitted, it should be made clear to recipients that opinions expressed by individuals are not those of the Company. Here are a few examples of corporate policies in use today:

- Company-provided Internet/Intranet and email privileges, like computer systems and networks, are considered company resources and are intended to be used for business purposes only. Employees should be aware that usage is monitored for unusual activity.

- Correspondence via email is not guaranteed to be private. Communications of a sensitive or confidential nature should not be sent unless they are encrypted.
- Corporate email accounts, Internet IDs and Web pages should not be used for anything other than corporate-sanctioned communications. It should be made clear to recipients that opinions expressed by individuals are not necessarily those of the Company.
- The distribution of any information through the Internet, computer-based services, email and messaging systems is subject to the scrutiny of the employer. The Company reserves the right to determine the suitability of this information.

Potential Legal Issues

- Visiting Internet sites that contain obscene, hateful or otherwise objectionable materials.
- Sending or receiving any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person.
- Uploading, downloading or otherwise transmitting commercial software or copyrighted material in violation of its copyright.
- Representing personal opinions as those of the Company.
- Using the Internet or email for gambling or illegal activities.

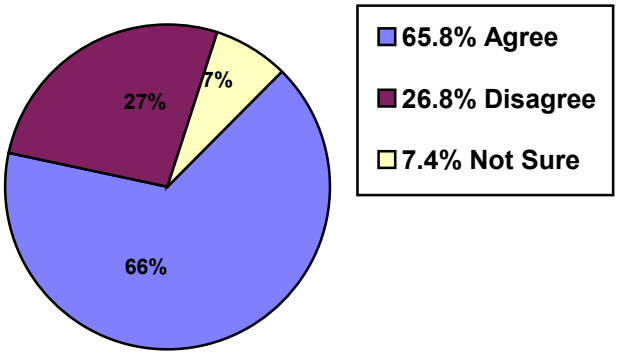
Security and Network Issues

- Use of the Internet/Intranet and email may be subject to monitoring for security and/or network management reasons.
- Downloading any software or electronic files without implementing virus protection measures that have been approved by the company.
- Intentionally interfering with normal operation of the network, including the propagation of computer viruses, or sustained high volume network traffic that substantially hinders others in their use of the network.
- Examining, changing or using another person's files, output or user name without explicit authorization.
- Other inappropriate uses of Internet/Intranet or network resources that may be identified by the network administrator.

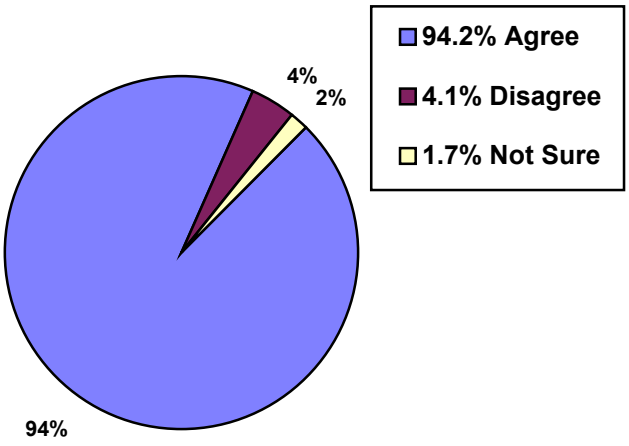
Implementing the IAP

In general, human nature dictates that people (employees) have a higher comfort level if they know the rules: they appreciate knowing the standards to which they are being held and the consequences for behaving otherwise. In other words, people like knowing what's expected of them and enjoy being able to successfully meet those expectations. In a PC World Online survey, most respondents agree that their employer has the right to monitor how they use the Internet connection at work-provided they know if the boss is peering over their virtual shoulder.

My employer has the right to monitor ...



... but I should be informed first.



Source: PC World Online survey, June 1997

It goes without saying that full management support—all the way to the top of the organization—is essential to implementing a successful IAP. Do whatever it takes to educate senior management on the finer points of your policy, and make sure they set a good example.

Know Who is Responsible

Whether the people responsible for enforcing your IAP are in Human Resources or in MIS, be sure that a responsible group or person is appointed and is fully aware of this responsibility.

Publicize It

The IAP should become part of your organization's overall policy manual. As with other company policies, you'll want to make sure it's readily available, widely disseminated and clearly understood by all. In fact, many organizations require that employees sign the IAP document as a condition of receiving Internet access privileges.

Be sure to clearly spell out who is covered by this IAP, whether it is some or all of your employees. If you intend the policy to cover all employees, say so.

Conduct Training

Training will ensure that your policy is understood by all. Training should be a prerequisite for Internet access, not only in the mechanics of using email and browsers, but in the ethical, legal and security aspects associated with participation in a global public network.

Employees should be reminded of the 'contract' you have with them: the covenant between company and employee is that the Company supplies the employee with needed tools and pays the individual. In return, individual employees work toward agreed-upon objectives. It's a breach of that agreement to spend significant time on the Internet doing personal activities.

Develop Guidelines for Enforcing the Policy

Extend your policy beyond initial guidelines. Develop a process for handling offenses within your organization; for example, what to do in the case of a 1st offense, 2nd offense, 3rd offense, etc. Clearly outline the consequences of non-conformance with your official IAP.

Choosing the Right Filtering Software

Just about anything you need to do to implement a viable IAP can be accomplished with existing technology. In fact, you'll probably find that there are several ways to get the job done.

First generation Internet access tools were designed to run on stand-alone PCs, and were mainly developed to protect children from objectionable content. Today's business solutions, such as SurfControl's SuperScout, are designed for network implementation. To decide what's right for your company, you need to consider several areas:

Flexible Monitoring

Your filtering software should enable you to implement any IAP you choose. Don't write your policy around constraints of limited tools, and what they enable you to do. Select one with the flexibility to help you enforce your policy— whatever it is.

You should be able to implement varying levels of filtering restrictions depending on the day of the week or the time-of-day: for example, it could be more stringent between 8am and 6pm, and more lenient after 6pm and on weekends.

You'll want to look for software that also lets you configure access by user and group; for example, you may want to give top management more access than others, or you may want to set up different levels of filtering for one department compared to another, due to specific job needs.

Complete Reporting

Graphs and reports will enable you to know when and how many sites not conforming to your IAP are requested, whether you choose to block them or simply monitor those requests. And once you've identified possible problems, you want to be able to track those users more closely and work with them to enforce the policy. So find out how many reports are available, whether you can customize them, and how the reports are distributed, such as by automatic email or an internal Web site.

Intelligent Filtering

The software should include a clear statement of the criteria used to block sites so you can answer any questions that arise internally, and be able to explain what is and isn't blocked and why.

Put the software to the test to ensure that blocked sites are sites that should be blocked, while access is allowed to sites that should not be blocked. Too many filtering packages "throw out the baby with the bathwater": it's easier to over-block than to block carefully and accurately, and that may result in the inability to access useful sites. The software filtering should enhance employee productivity, not frustrate users trying to work.

Regular Content Updates

The Internet grows every hour. Some reports suggest that each day, 10,000 new Web pages come online. You should be able to update frequently — even daily if you choose to—to ensure up-to-date protection against newly posted sites.

High Scalability and Strong Performance

The software should be able to handle thousands of users, so you can run the monitoring easily from one location on your network. And it should be able to handle thousands of users without affecting network performance. Investigate supported network topologies, servers, and firewalls to make sure the software will both be able to work with your network and handle the number of users.

Reliable Support

An established vendor will be there to support you in the future, as your company grows. Look for a technically strong, well-respected company with extensive knowledge of the Internet that gives it staying power.

Summary

You will definitely want to have an IAP in place as you roll out Internet access throughout your organization. Here's why:

- **Increase employee productivity**

  The amount of time employees spend "surfing the Internet" for personal reasons has been shown to decrease if they know that Internet access is being monitored.

- **Enhance network bandwidth**

  Non-productive sites consume a significant amount of bandwidth. When employees are downloading heavy graphics (gif and tif files), audio clips and other non-work-related information, this puts a drain on the company's limited bandwidth (an expensive resource) and causes a slowdown in network performance which impacts the rest of your employees who are trying to get some work done via the Internet.

- **Reduce legal liability**

  Just having an IAP for the Internet that specifically states that employees should not be viewing sexually explicit sites, hate speech, violence and other highly inappropriate materials will strengthen your company's position greatly if there should ever be charges of allegedly creating a hostile work environment.

We do not want to dictate or intend to influence what your policy should be. You alone can decide on the best approach given your current workplace environment, company goals and corporate culture. Your company may decide to take a very liberal or a very conservative stance on the use of the Internet within your organization. You are in the best position to judge. Either way, it is extremely important to develop a policy, publish it and stand behind it.

Contact Us…

This guide has been provided to assist you in the process of developing your IAP. Just as it is good business to have a policy in place, we also recommend that you choose one of the SurfControl products or technologies to uphold your IAP – whatever it entails. Please feel free to call us for more information about the benefits of bringing Internet content monitoring and filtering software into your organization. For more information or to download a FREE 30-day trial version of SuperScout:

Visit: www.surfcontrol.com
Call: 1-800-368-DEMO (3366)
Email: surfsales@surfcontrol.com