# [The Importance of Internet Usage Policies](http://www.techrepublic.com/article/the-importance-of-internet-usage-policies-6071808/)

You provide Internet access to employees to hopefully allow them to be more productive. This article shows why it's important to have an internet usage policy on hand so users know what they can and cannot do on the Internet.

By [Erik Eckel](http://www.techrepublic.com/search/?a=erik%2Beckel) | August 24, 2006, 12:00 AM PST

Powerful tools require careful management. They always have. The same power and force that make a tool so effective can, in a single moment of inattention, quickly transform the tool from an implement of construction into a device of destruction. The maxim holds true whether the subject is a contractor-grade 7 1/4-inch circular saw or the Internet.

The same capacities and dynamism that make the Internet such a profound business tool also render it a potentially dangerous diversion. Used improperly, the Internet can subject every organization to harassment claims, countless hours of lost productivity and innumerable security leaks and vulnerabilities.

**Eight seconds to infection**

Industry statistics demonstrate that PCs connected to the Internet possess an incredibly high likelihood of quickly being afflicted with spyware programs and viruses. The malicious programs can, subsequently, result in data corruption or worse, the organization's data being made available to unauthorized parties as the result of a Trojan horse infection.

In fact, a BBC [report](http://www.bbcworld.com/content/clickonline_archive_14_2005.asp?pageid=665&co_pageid=3) claimed Windows XP machines were infected with a virus within eight seconds of being connected to the Internet. According to another[story](http://money.guardian.co.uk/internetcosts/story/0,,1656322,00.html), unprotected systems connected to the Internet have "a 90 percent chance of becoming infected with a virus within 40 minutes." Most corporate systems will enjoy antivirus and firewall infection, but risks still exist.

**Billions in lost productivity**

Employees frequently review eBay auctions, check sports scores, read titillating entertainment news and trade stocks, all when they should be fulfilling job tasks. Numerous studies place the cost of lost productivity resulting from improper Internet use in the billions of dollars range. Outplacement consulting firm Challenger, Gray & Christmas, Inc. [estimates](http://www.foxnews.com/story/0,2933,188043,00.html) that the NCAA's 2006 college basketball tournament alone cost employers $3.8 billion in lost productivity as a result of employees viewing games online.

If such figures seem extreme, even conservative estimates prove alarming. Consider the effects of each employee (in a 100-employee organization) wasting just 20 minutes a day on unauthorized Internet use. At just $40 an hour, that's more than $340,000 in lost productivity a year.

**Legal liability**

Still other employees may surf inappropriate adult sites that, if enabled by management and witnessed by others, could constitute grounds for harassment claims. Or, employees using organization-provided Internet access could knowingly (or unknowingly) violate international copyright law, which could further expose the organization to liability.

**Internet usage policies**

What's an organization to do? Internet access is now required for fulfilling job responsibilities seemingly in a majority of professions. While various technology solutions (proxy servers, Web monitoring software, filtering appliances, firewalls, etc.) can help prevent users from misusing the Internet, no technology is foolproof. Users encumbered with no other restrictions are likely to find success circumventing strictly technological controls.

That's where the value of an Internet usage policy, also known as an acceptable use policy, comes into play. Regardless of the technological solutions in place, a policy ensures every employee and organization representative understands organization-provided Internet services are to be used only for fulfilling job responsibilities.

Further, Internet usage policies can:

* Clarify what constitutes acceptable use of Internet services.
* Ensure employees understand who to contact with questions regarding acceptable use.
* Ensure employees understand the penalties that arise from Internet misuse.
* Help lessen an organization's spyware and virus infestation rates.
* Provide human resources with signed documentation from each employee stating a pledge not to improperly use Internet services.
* Help mitigate productivity losses.
* Decrease dependence upon technology solutions used to enforce employee behavior.
* Reduce the organization's liability resulting from harassment claims, copyright violations originating onsite and other illegal acts.

Complete TechRepublic's Internet Usage Vulnerability Assessment if you are unsure whether your organization requires an Internet usage policy. The interactive Microsoft Excel tool will help gauge your organization's exposure.

Should the assessment convince you that your organization requires an acceptable use policy, review TechRepublic's Internet Usage Policy, which serves as a ready-made template. Customize the policy to meet your organization's specific needs, or use it as-is to quickly introduce an overarching policy within your organization.

Remember that just rolling out such a document will not eliminate the risks Internet use poses within your organization, however. The Information Technology department must aggressively enforce such policies. Employees will naturally resist the effort, so it is important to communicate the seriousness and the risks the policy is designed to protect against.