

# GFI WHITE PAPER

## THE IMPORTANCE OF AN ACCEPTABLE USE POLICY

In an ideal world, employees would use the computers and Internet access provided their employer solely for business use. It is however, sadly, not an ideal world. Throughout the work day, companies, schools, libraries and other organizations are exposed by their users to the misuse of the system. The dilemma faced by every company is what to do about it and how to start. In this White Paper we examine both the extent of the problem of misuse, and the role the creation and dissemination of an Acceptable Use Policy (AUP) can offer in helping an enterprise avoid unwanted consequences and enabling it to deal with transgressions in a fair and systematic way that will survive legal challenges without reducing employee morale and productivity.



### The extent of misuse

According to a survey by International Data Corp (IDC), 30 to 40% of internet access is spent on non-work related browsing, and 60% of all online purchases are made during working hours. The data IDC uncovered includes:

- 70% of all web traffic to Internet pornography sites occurs during the work hours of 9am-5pm.
- 58% of industrial espionage is perpetrated by current or former employees.
- 80% of computer crime is committed by "insiders". They manage to steal \$100 million by some estimates; \$1 billion by others.
- 48% of large companies blame their worst security breaches on employees.
- 64% of employees say they use the Internet for personal interest during working hours.
- 70% of all Internet porn traffic occurs during the nine-to-five work day.
- 37% of workers say they surf the Web constantly at work.
- 90% of employees feel the Internet can be addictive, and 41 percent admit to personal surfing at work for more than three hours per week.
- 25% of corporate Internet traffic is considered to be "unrelated to work".
- 30-40% of lost productivity is accounted for by cyber-slacking.
- 32.6% of workers surf the net with no specific objective; men are twice as likely as women.
- 27% of Fortune 500 organizations have defended themselves against claims of sexual harassment stemming from inappropriate email.
- 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the previous 12 months, 80% acknowledged financial losses due to computer breaches, 44% were willing and/or able to quantify their losses, at more than \$455 million.

### Solutions

One solution to the problem, beyond simply disabling the connections or depending on sometimes unreliable URL blockers, is to use Internet monitoring systems (see [GFI whitepaper](#)). According to IDC,

- 77.7% of major US companies keep tabs on employees by checking their e-mail, Internet, phone calls, computer files, or by videotaping them at work.
- 63% of companies monitor workers' Internet connections and 47% store and review employee e-mail.

### Acceptable Use Policy

While monitoring has been an effective tool in identifying abusers and cyber-slackers, Human Resources experts, as well as the courts agree that it needs to be accompanied by evidence of a "duty of care" intended to reduce unacceptable employee activity. A key aspect of this is what is commonly referred to as an Acceptable Use Policy.

Nearly every enterprise has a specified set of rules, usually spelled out in an employee handbook that an employee has to acknowledge by signature that he or she has read and understood. Some of these policies, such as that against racial or religious discrimination and mandatory email archiving are required by law or regulation. Other may reflect common business ethics or a particular company's culture such as prohibitions against drinking, unexcused absences, sexual harassment and the like. Policies also include a



set of sanctions that can be used against persons who violate the company's policies. They also provide a legally defensible basis for disciplinary action, up to and including termination.

One key advantage to policies like this is that while, traditionally, employers have been held responsible and liable for their actions in the workplace, the presence of policies prohibiting such actions has served as a liability shield that can completely or partially protect that company from lawsuits arising from employees acting in contravention of the policies.

To safeguard its electronic communications, every company, large or small, should have an Acceptable Use Policy in place that governs Internet, email and computer use in the business.

In essence, an Acceptable Use Policy serves as guidance for staff and volunteers on the behavior and use of technology that is approved by the organization. The policy should also detail the consequences that company personnel can expect to face for the abuse of this technology.

### **What should be in an Acceptable Use Policy?**

As discussed earlier, monitoring voice mail, e-mail and Internet use is generally legal, provided the employer has created and effectively communicated an Acceptable Use Policy. While the exact wording of the AUP will vary from company to company, there are some general guidelines on how an organization communicates such policy to its workers.

The key goal of an AUP is to eliminate any employee expectations that these means of communication or use of computers, email and the Internet at work are confidential. The policy must be non-discriminatory and it should prohibit all forms of non-business related communications. To this end, the policy informs employees that the employer may access, search and monitor voice mail, e-mail or company files of any employee that are created, stored or deleted from company computer systems. The policy must be uniformly enforced through employee education, ongoing monitoring and appropriate discipline. Obtaining prior consent will generally protect employers from liability.

Ideally an AUP should do the following:

- Define what systems are covered by the policy, e.g., voice mail, e-mail, Internet, and computer systems and files.
- Specify that an employer's computer systems are for business purposes only, and all files and messages are company property.
- If the company chooses to allow some personal use, the policy should caveat this by forbidding personal use that interferes with an employee's work or that of others (e.g., prohibiting non-work related websites such as chat rooms, games, travel, shopping, stock trading, hate/discrimination, pornography, etc.).
- Specifically ban transmitting or downloading of material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic or obscene.
- Prohibit copying and sending any confidential or proprietary information, or software that is protected by copyright and other laws protecting intellectual property.
- Prohibit unauthorized access by employees of other employees' electronic communications.



- Warn employees that any misuse will be subject to discipline, up to and including termination.
- Advise and emphasize employees that they have no right to expect that their communications or use of employer's computer information systems is either confidential or private.

After the AUP is drafted, organizations should require the employees to sign the AUP. Some companies have also taken the further step of installing an on-screen warning about their electronic communications policy that appears every time employees log onto their computers.

### Summary

Misuse of the Internet, email and computers in the workplace represents a serious and growing challenge to every organization, regardless of size. In addition to potential illegal activity, disclosure of company secrets, and introduction of malware, misuse of these systems has a real dollar cost in terms of lost productivity. To date the most successful means of combating this has been through monitoring, by a variety of means.

The first step in any organization's defensive measures against abuse is a prior consent statement, commonly referred to as an Acceptable Use Policy that specifies that employees have no right to an expectation of privacy with respect to their use of business computers, email systems and Internet connections. The AUP also details unacceptable activities, specifies sanctions, advises of the potential for monitoring and places responsibility for inappropriate behavior on the employee who transgresses those rules. The AUP should be widely disseminated and employees required signing and acknowledging their understanding of it. In addition to providing employees throughout the organization with clear definition of the organization's expectations, a properly executed AUP can serve as a liability shield for the organization in the event of misbehavior by an employee, as well as a legally sanctioned basis for disciplinary actions, including termination.

© 2010. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.