Your Internet Acceptable Use Policy

It is essential that every company has an Acceptable Use Policy, which explains to staff what they may and may not do in the course of accessing the Internet for business purposes. We outline how to develop and maintain your AUP.

By Dave Stott
IT Journalist

Most organisations can appreciate the considerable benefits of allowing their users to access the Internet. Not only does it mean that they can make use of global email but it also means that they have a wealth of information available to them at the touch of a button. The Internet can provide a valuable resource for all types of research and information gathering, indeed access to the Internet is seen by some users as a mandatory requirement in order for them to perform their job.

When it comes to accessing the Internet the majority of users adopt a fairly sensible and responsible attitude. They will not download and distribute pornographic images or dubious programs which may contain viruses, or subscribe to racially offensive newsgroups. Generally they can be left to their own devices and will only make use of their Internet connection for genuine work-related purposes. Unfortunately, this doesn't always apply to every user and some will occasionally make use of their Internet connection for their own personal purposes.

The two most common reasons for staff misusing their company Internet connections are: because the work connection is faster than the home one, thus useful for downloading large files; and because some things can't wait until after work, eg, online trading of stocks and shares.

The Dilemma

Technical support engineers often face a rather tricky dilemma. Allowing your users complete freedom to use the Internet as they please gives them enormous benefits but it is also fraught with potential problems. For example, browsing the Internet

This Internet Acceptable Use Policy (AUP) shall apply to all employees of the company, contractors, agents, consultants and guests who may be utilising company resources for Internet access.

General

Access to the Internet is granted on the basis that it is used solely for the purpose of conducting company business and that it supports the goals and objectives of the company and its various business units. The Internet is only to be used in a manner that conforms to the existing company standards for conducting business and as part of the normal employee job responsibilities.

Email accounts and other forms of Internet information exchange, such as chat rooms, file transfer and Web page publishing should only be used for sanctioned business communications purposes.

The use of the Internet (browsing, file transfer and email) will be monitored randomly to ensure security and conformance to the AUP. The company reserves the right to restrict or completely prohibit Internet access if it feels that security has been compromised or that the AUP has not been adhered to.

Distribution of any information via the Internet is subject to scrutiny and the company reserves the right to determine its suitability or otherwise.

The use of the Internet by users is subject to this country's laws and any illegal use of the Internet will be dealt with appropriately.

Figure 1 - A sample Internet AUP.

for personal use can be detrimental to employee productivity, can effect network performance, compromise network security, and expose your organisation to potential litigation or even criminal prosecution.

You often need to tread a fine line between complete freedom and taking total control over who has access to what on the Internet. One thing that can help resolve the situation is the implementation of an Internet Acceptable Use Policy which clearly states precisely how users should make use of their Internet connection and what they should and should not do whilst online in company time.

AUP Goals

The concept of an AUP is to define a set of rules and guidelines which will help your users understand their obligations when using the Internet. As a result, one of the primary goals of an AUP is to make users aware of the consequences of their own actions when online. Ignorance is really no excuse and an appropriate AUP should be used to inform users of their responsibilities.

The fact that a company or organisation has an appropriate AUP can shield them (to some degree) from potential liability for things like copyright infringement or email abuse (spamming) by their employees.

An AUP should be an integral component of an organisation's security policy. One of its goals should be to promote security awareness and good practice. Also by promoting an effective AUP you will go some way towards encouraging the proper

You must not:

- visit Internet sites that contain obscene, racist or other offensive material;
- make or post obscene, indecent, racist or offensive remarks or comments on the Internet, nor should you entice others to do so;
- solicit email or other Internet-based services which are not directly related to the running of the company or which are for personal gain;
- transmit any material that is defamatory or which is intended to offend, annoy, harass or intimidate another person or persons;
- express any personal opinions as being representative of the company, whether in private email or in public areas such as Usenet;
- upload, download or transmit any copyrighted materials belonging to parties outside the company and any company material which may be subject to future or pending copyright;
- publish or otherwise reveal any commercially sensitive, confidential or proprietary company information including but not limited to: financial data, research and development information, marketing plans, customer details, internal memos, minutes of meetings, management reports or business operation details;
- send any confidential email without using the appropriate encryption procedures;
- download any software or other electronic files without utilising the appropriate company approved virus protection measures and procedures;
- intentionally interfere with the normal operation of the company network by downloading excessively large files or making use of streaming video or audio feeds;
- alter or in any way change the headers associated with emails or attempt to gain access to information for which you are not authorised;
- make illicit use of another user's ID and password in order to circumvent company security policies;
- attach a modem to your PC in order to gain direct and unmonitored Internet access.

You must:

- make use of your Internet access in a judicious and considerate manne;
- ensure that all email contains the company approved disclaimer (see Figure 3);
- ensure that every precaution is taken to protect the company's reputation and good name;
- report any breaches of the AUP by any member of staff to the appropriate manager.

Failure to follow the company's Internet AUP will result in disciplinary action and could result in termination of employment. The company also reserves the right to report any illegal or criminal violations to the appropriate authorities.

"Failure to follow the company's Internet AUP will result in disciplinary action and could result in termination of employment."

Figure 1 - A sample Internet AUP (Continued).

and positive use of Internet resources. Most importantly, an AUP will specify the company policy as to what is acceptable use of the Internet and what is not.

Development

Granting and enabling users access to the Internet can be a rather emotive subject. Many users feel that they have an absolute right to unfettered Internet access. Others may not be willing to accept the responsibility associated with self-disciplined access. Similarly some may be fearful that their privacy may be compromised and may even request that an AUP be implemented in order to protect themselves.

Users' concerns and realistic requirements need to be taken into account. As a result an AUP should not be formulated in isolation. Neither should it be created solely by the IT department. Instead you should instigate a consultation process with all the appropriate members of staff. In a large organisation it is often not practical to canvass everyone's opinion, in which case you should seek to gain a representative sample of typical users from each department. Setting limits as to what a user can and cannot do should be agreed via mutual discussion between the relevant parties. Therefore you need to consider involving senior management, business unit managers, human resources (personnel), the legal department and representatives of the various user groups in the process of defining and developing your AUP.

Bear in mind that Internet access doesn't have to be "all or nothing" and you need to be fairly flexible in your approach to granting access. You need to consider which Internet services (email, browsing, ftp etc), the type of access (full, partial or none), access periods for both work-related and personal access (if applicable), and any sanctions that will be applied in the event of a user breaking the rules. Internet access should be granted as a privilege which if necessary can be revoked.

Many of these conditions will already be applied to your existing network and you can think of the Internet AUP as an extension to the management and control that you currently apply to your internal systems.

- Have any new staff joined the company and are they fully aware of the AUP and its ramifications?
- Has there been any feedback from users regarding any possible problems or shortcomings with the AUP?
- Is the AUP having any adverse effect on normal day to day business operations?
- Is your email disclaimer (see Figure 3) up to date and does it provide sufficient protection for your company?
- Have you revoked the Internet access privileges of any staff or contractors who have left?
- Have there been any incidents, such as breaches in security that require a change in policy or monitoring of Internet access?

Figure 2 - Considerations for maintaining the AUP.

The information in this email is confidential and may be legally privileged. It is intended solely for the addressee and access to the email by anyone else is unauthorised. Accordingly any dissemination, copying or other use of this message or any of its content by any person other than the Intended Recipient may constitute a breach of civil or criminal law and is strictly prohibited. If you are not the Intended Recipient, please contact the sender as soon as possible.

Figure 3 - Sample email disclaimer.

Excuses

As mentioned previously, ignorance is no excuse for failing to abide by the rules of an AUP. However, you may need to consider providing additional training to ensure that users understand the potential problems associated with Internet access. Additional training may be required to encompass things like file downloading, browser plug-ins, telnet, cookies and Web page cacheing.

If your company policy is to allow users to make use of their Internet connection for personal needs then the AUP defines precisely the level and times when personal use of Internet access is allowed. It's no good simply saying that users can do what they like when they are not busy as this degree of freedom is likely to be abused. The AUP should specify precise times when personal access to the Internet will be permitted and should take into account the general network traffic loads during normal business hours.

Users will need to be assured that their personal privacy will be maintained and that the AUP will not contravene their basic employment rights. This can be a delicate issue as the organisation needs to both protect itself in terms of maintaining the confidentially of things like business plans, marketing strategy, financial results and at the same time monitor authorised user access to relevant information.

The AUP should clearly state to which users of the Internet the policy applies and any possible exceptions. Details of any sanctions or consequences for users that do not conform to the AUP should be clearly defined.

Example AUP

As a guide to what a formal AUP should look like, Figure 1 is an example of a typical policy. This provides a basic outline for a typical company policy. It does not cover every eventually but can act as a template for your own Internet AUP. If you're looking for further inspiration, do a Web search for "acceptable use policy" and you'll find links to hundreds of company policies which are, for one reason or another, available for public scrutiny.

Monitor And Control

A suitable AUP can provide your users with a formal rule book for accessing the Internet but, as with any set of rules, adherence generally relies on trust. Therefore you need to consider various tools and utilities which can help you monitor and enforce the AUP rules.

Start, of course, with standard security measures such as firewalls, virus scanning and content filtering in order to protect your organisation from wilful hacking or damage to company data. When it comes to policing user access to the Internet you have basically two choices. First, you can simply monitor all access to the Internet and hopefully identify any breaches to the AUP and then take action accordingly. Products such as Sessionwall will do this for you.

You may wish to consider using a Web proxy server to allow you to monitor which of your users are accessing which Web pages. Similarly, if you are running your own mail server you can check all incoming and outgoing email. However, monitoring access can be extremely time consuming and there is always the danger that you will simply miss something important due to the high level of Internet traffic that requires monitoring.

Second, and by far the best option, is to use access control software to prevent users from actually visiting specific Internet sites or to filter the content being sent and received. There are numerous packages available that can be used to control and manage Internet access. Many will allow you to create a blacklist of dubious sites and to control and manage the amount of bandwidth available to Internet users. Some packages will even let you vary the level of filtering based on particular days of the week or time of the day. Here the most important thing is flexibility and any package should enable you to implement any of the requirements of your own particular AUP.

Maintaining The AUP

Once you have implemented an appropriate AUP it is vital that you maintain and update it regularly. You need to take into account changes in staff, business practices, management expectations and developments in Internet technology. Therefore you should undertake periodic reviews of your AUP and make any adjustments and modifications accordingly. Figure 2 lists some of the things that you might need to consider.

Quite simply your AUP should not be considered as a fixed set of rules or guidelines and needs to be both flexible and dynamic in nature. The Internet changes so rapidly that you need to keep on top of things or you run the risk of being overtaken by events and developments.

Conclusion

Developing and implementing an appropriate AUP for your company or organisation will go some way towards effectively managing user Internet access. However, it is not a general panacea and needs to be a component of your overall security and management procedures. The simple fact that you have an Internet AUP will make users aware that they do not have *carte blanche* when they are online and that they are ultimately responsible for their actions.

If you haven't got an Internet AUP then don't put it off, do something now. You should formulate and implement even the most basic policy before it is too late.

PCSA

Further Information

There are plenty of commercial and shareware (or even freeware) packages and tools that can help you implement and maintain an Internet AUP. In addition, there is lots of general information about controlling and managing Internet AUPs available. The following are some pointers to online resources:

http://www.surfcontrol.com/

http://www.squidguard.org/

http://www.languard.com/languard/languard.htm

http://www.dms-soft.com/index.htm

http://www.webattack.com/shareware/security/swaccess.shtml

http://www.websense.com/index2.cfm

http://www.rulespace.com/

http://www.info-law.com/guide.html

http://www.saferinternet.org/

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.