Peer Reviewed Article Vol.10(4) December 2008

Hierarchical analysis of acceptable use policies

P.A. Laughton
Department of Information and Knowledge Management
University of Johannesburg
Johannesburg, South Africa
paull@uj.ac.za

Acceptable use policies (AUPs) are vital tools for organizations to protect themselves and their employees from misuse of computer facilities provided. A well structured, thorough AUP is essential for any organization. It is impossible for an effective AUP to deal with every clause and remain readable. For this reason, some sections of an AUP carry more weight than others, denoting importance. The methodology used to develop the hierarchical analysis is a literature review, where various sources were consulted. This hierarchical approach to AUP analysis attempts to highlight important sections and clauses dealt with in an AUP. The emphasis of the hierarchal analysis is to prioritize the objectives of an AUP.

Key words: Hierarchical, AUP, analysis, legal

Received 16 July 2008

Contents

1 Introduction

Acceptable use policies (AUPs) are often not seen as proactive tools in the prevention of misuse of computer facilities. AUPs work in conjunction with active tools such as content filters in ensuring correct use of computer facilities, but AUPs also have a bigger role to play in the organization. To block unwanted online content, a thorough AUP needs to complement the active tools employed, thus ensuring continuity. AUPs can be seen as a passive form of control; while they do not physically restrict a user from inappropriate online behaviour, they rather act as a guideline. Many studies support the argument that AUPs and content filtering systems can effectively deter and prevent the misuse of computer facilities (Chen, Chen and Yang 2008).

AUPs are divided into different sections, making it easier to understand and follow, thus allowing for continuity. Each section of an AUP identifies a different focus area. An AUP should include a section on the disciplinary action that will be taken against those who are caught misusing the computer facilities provided.

AUPs are under constant fire from those attempting to access disallowed content or use facilities for non-work related purposes. It is vital that careful consideration goes into the development of an AUP. For this reason AUP evaluation serves as an analysis tool to identify strong and weak points in current AUPs ensuring more effective AUPs.

There are several approaches to AUP analysis. The hierarchical analysis of an AUP was developed from a literature review in which various sources were consulted to determine an order of importance for AUP content. In recent times, organizations seek to reduce Internet abuse by taking the necessary precautions (Chen *et al* 2008).

This research attempted to create a hierarchical analysis of AUPs. In the literature review under taken for this research various sources (Flowers and Rakes 2000; Kelehear 2005; Scott and Vass 1994; Simbulan 2004; Surfcontrol 2005) were consulted, where essential content was identified for the construction of the hierarchical analysis. This hierarchical analysis led to a unique structured approach to AUP analysis.

1.1 Research problem

AUP analysis is essential for identification of strengths and weaknesses of an AUP. The following research problem was identified: *What focal areas should be dealt with, in a hierarchical analysis of an AUP?*

1.2 Sub-problems

To solve the research problem, the following sub-problems were addressed:

- What is an AUP
- Why is it necessary to have an AUP?
- What content should typically be included in an AUP?
- What is a hierarchical analysis of an AUP?

top

2 Defining acceptable use policies (AUPs)

There are many different policies pertaining to the acceptable use of facilities. For the purpose of this research article, reference is made to that of the computer facilities provided by an organization. This includes the physical hardware resources, and use of intranet and Internet applications. This theory is applicable to any organization that allows personnel and

members access to the Internet and other computer facilities.

An AUP is a formal or informal document, used to organize computer and information resources, defining unacceptable use as well as the consequences for non-compliance to the policy (Simbulan 2004). AUPs are created with three main goals:

1. Educating users about activities that may be harmful to the organization
2. Providing legal notice of unacceptable behaviour and the penalties for such behaviour
3. Protecting an organization from liabilities it may incur from misuse of the Internet and other computer facilities.

According to Scott and Vass (1994), an AUP is used to define who can use computer facilities and for what purpose. An AUP acts as an organization's official voice on ethical use of computer and Internet facilities. Thorough AUPs are well organized and easy to read.

The Net Dictionary (2004) identifies an AUP as a set of rules that govern the network and how it may be used. It acts as a set of rules applied to networks (two or more computers linked with the use of a communication protocol) to restrict use. Common practices include new members joining an organization to sign an agreement regarding the AUP before access is granted to the computer facilities. An AUP needs to be concise and clear (Wikipedia 2005).

Organizations customize their AUP to fit their specific needs based on unique factors. AUPs can vary in length from one page to more then ten pages. AUPs can be divided into two categories: broad policies and detailed policies. Broad policies are easier to digest but leave grey areas, causing debate. Detailed policies ensure that there are no questionable clauses. Policies should find a balance between being too vague and too technical. It is very easy to fall into a trap of over policing the use of computer facilities and the Internet (Kliener and Welebir 2005). A study by Seymour and Nadasen (2007:553) revealed that the AUPs in their survey sample were not comprehensive and major abuse was omitted.

top

3 Importance of an AUP

Many organizations have not carefully considered the importance of an AUP. It is important that facilities provided are used with good intent, but the importance of computer facilities usage is often overlooked, leading to inappropriate and outdated AUPs. The most important reason for an organization having a well-planned AUP is to avoid any legal complications that may be encountered through the misuse of the computer facilities provided, either by personnel or a member of the organization.

3.1 AUPs as a legal policy

Granting personnel and members use of the Internet can lead to their viewing inappropriate content, including sexually explicit, racist and violent content. These activities can put legal pressure on an organization, leading to possible criminal prosecution. Organizations as well as their members need to be protected by promoting responsible Internet use (Surfcontrol 2005).

In Germany, the former head of Compuserve was charged for failing to block access to pornography. Although Compuserve argued that it is almost impossible to filter all content and monitor thousands of files, a charge was still laid. The convicted received a two-year probation period and was fined a large sum, payable to charity (Held 1999). This ruling made

those with the responsibility of controlling Internet usage legally liable. Incidents like this can be avoided if the correct procedures are in place.

It is vital that an organization is fully aware of the relevant laws and standards before developing an AUP. Essential research in issues dealing with laws on Internet usage (cyber laws) and netiquette need to be carried out before final drafts of an AUP are compiled. In addition, all computer users must be notified of any activities that may be newly classified as unlawful Internet activities; Internet law is a dynamic field, with numerous new cases brought to trial, creating new precedents (Lichtensten and Swatman 1997).

top

4 Key issues AUPs need to address

ccording to Surfcontrol (2005), the goals of an AUP should clarify the organization's policy regarding the usage of the Internet and other computer facilities. An AUP is vital to an organization for the protection from potential liability, to avoid security threats by promoting awareness and good practice, and for encouraging positive use of the Internet as well as other computer facilities provided.

According to Kelehear (2005:33) the following key points need to be addressed in an AUP:

- Statement on the intended use and an outline on the advantages of the Internet
- List of responsibilities for users
- Code of conduct administering the use of the Internet
- Description of what constitutes acceptable and unacceptable use of the Internet
- Disclaimer absolving the organization from possible responsibility of any misuse of the Internet.

An AUP should strive to be a well-rounded policy taking into consideration the rights of the users. An AUP needs to be concise and fair when addressing Kelehear's (2005) key points. These key points highlight the core of an effective AUP.

Once an appropriate AUP has been implemented, regular updates are essential. Organizations need to take into account changes in staff, business practices, management expectations and developments in Internet technologies. Owing to the dynamic nature and structure of the Internet, regular updates are needed to avoid any potential risks (Stott 2001).

top

5 Recommendations for developing and planning an AUP

Many points need to be taken into consideration when planning and developing an AUP. It is crucial that careful consideration be given to all influential factors pertaining to the organization in question. A well-rounded policy is carefully planned and includes input from and consideration by all parties involved including staff, members, legal representatives and external experts.

It is common practice to start with a brief policy overview when designing an AUP. This serves as an introduction to personnel and members on how resources on the Internet and intranet can be used as a productive resource. This introduction overview should explain why an AUP is necessary.

AUPs need to address areas around security. A disclaimer in the security section of an AUP

should outline the consequences for persons attempting to circumvent any of the security measurers in place. The organization needs to secure information systems from any unwarranted external penetration, which could lead to the leakage of valuable competitive information.

So many AUPs are confusing and written as if they were specifically targeted at lawyers and legal professionals. A confusing or murky AUP will be less effective, creating a sense of ambiguity. People will not be able to digest an AUP if it is not simply constructed, logical and consistent. The correct use of grammar should be emphasized in aid of reducing ambiguity (Kinnaman 1995).

Wording of an AUP should be carefully considered. This is an example of a popular clause, written without consideration: 'Anybody found trying to enter an objectionable Website will have their Internet access lifted'. However, experienced Internet users know that one cannot be completely certain of the nature of the Website until it is opened in the user's browser as URLs and links are not always indicative of the type of content on a site. Issues such as these need to be taken into consideration.

5.1 Seven Ps model

Scott and Vass (1994) developed the seven Ps model, which identifies different points and issues that need to be addressed in the drafting and implementing of an effective AUP. The seven Ps are: participation, partitioning, philosophy, privacy, pernickety, phog phactor and publication.

1. Participation: An AUP should be compiled by a broad committee selected from all groups of users. These groups should include administration, students, facilities, clerical staff, IT and computer personnel.
2. Partitioning: An AUP should be divided into several logical sections, each of which deals with a specific problem area. These partitioned areas should cover a generalized central policy, linking to sections dealing with common problems such as security, privacy, copyrights and the Internet.
3. Philosophy: An AUP needs to be in line with and emphasize the mission statement (broad policy) of the organization. There should be a common theme carried throughout the document. The AUP should identify how permissive an organization may be with regard to religion, business, political and civil activities.
4. Privacy: All users need to understand what degree of privacy is acceptable. An AUP should clearly state when it is acceptable to breech the privacy agreement in order to protect the organization and personnel or members from harmful use.
5. Pernickety: This section consists of a list of do's and don'ts, making up the core of the AUP. It covers issues such as privacy, hacking, illegal content and punishments for violations. It is vital that this section is not overly long with detailed descriptions of various disciplinary actions. On the other hand a short, incomplete AUP lacks specific guidance and can encounter possible problems with enforcement.
6. Phog Phactor: Because of complicated legal jargon, AUPs tend to be hard to understand and read. Compilers of AUPs need to utilize techniques for improving readability.
7. Publication: This deals with the means an organization uses to communicate its AUP. From a legal perspective, an AUP needs to be disseminated in such a way that the use of an organization's computer facilities are legally bound. Some methods for publication include printed copies of an AUP, visible in areas where computer facilities are located. Another way of ensuring agreement is by making users agree to the terms of the AUP before they are allowed to logon and access various online resources.

Scott and Vass's seven Ps model is useful in identifying focal areas of an AUP. This basic model will help assure that organizations remain protected from common threats, but more detail is necessary to compile a thorough AUP. This model emphasizes the need for an AUP to be in line with the mission statement and philosophy of an organization.

5.2 Tips for effective AUPs

Hughes (2004) identifies steps that need to be taken to create an effective AUP. These steps act as guidelines. Firstly, a policy review needs to be conducted before any tasks are completed. The policy review will enable the organization to distinguish between the different network access permissions. Different policy controls may apply to different individuals or user groups in the organization, as not everyone needs to have access to the Internet and possibly other resources residing on the computer network. Monitoring network traffic is useful for identifying and monitoring specific areas or groups that engage in inappropriate or unnecessary online behaviour.

All parties need to be consulted to ensure that established policies match the ability of the Internet infrastructure to support all parties involved. A policy test exercise with key members should be conducted at the draft stage. The organization should ensure that the policy is practical in terms of achieving objectives and at the same time that it is flexible enough to accommodate change resulting from possible emergency situations.

All possible loopholes need to be considered. A legal team should be involved with the review of the policy; this is an ongoing task as new laws are constantly being passed. Any changes in the policy need to be announced and communicated. A plan should be implemented to effectively communicate any changes to personnel and members (Huges 2004).

top

6 Evaluation criteria for AUPs

There are different approaches that can be used to evaluate AUPs. Evaluation of an AUP is crucial for the identification of strengths and weaknesses in current AUPs. Evaluation criteria can also be used for designing a new AUP. Common themes are analysed through an evaluation process. A strong emphasis is placed on whether or not the AUP is technically and legally correct; the policy should not have any loopholes. Different AUPs have unique focus areas.

Listed below are two sets of evaluation criteria: Flowers and Rakes's four area approach and a hierarchical analysis of AUPs.

6.1 Flowers and Rakes four area approach

Flowers and Rakes (2000) developed an approach to analyse AUPs that concentrates on four areas: liability issues and concerns, online behaviour, system integrity issues and concerns and, lastly, the quality of content on the Internet.

The area of liability issue and concerns is further divided into three categories: service liability, damages and the costs incurred by the users, as well as content quality and accuracy.

1. Service liabilities investigate services such as email, information and news services, public domain, shareware software, discussion groups and any connection to library

services. Disclaimers for these services imply that the accessibility to these services might be interrupted or with errors.
2. Damages and costs incurred involve the actual cost of damages that a user might incur while using the Internet. A disclaimer would emphasize that the organization would not be held responsible or liable for any direct, indirect, incidental or consequential damages sustained in connection with or during operation of the Internet.
3. Quality and accuracy of content on the Internet are other areas that an AUP should address by exempting the organization from any responsibility for content published on the Internet.

The second area deals with the online behaviour and netiquette required by the organizations. This outlines issues and concerns addressing behaviour of system users. Typical content in this section would state the appropriate manner in which to conduct online activities such as emailing and surfing the World Wide Web (WWW). Inappropriate behaviour is defined as actions such as the violation of copyright laws, use of the system for community, political or religious reasons, violation of privacy, use of the computer facilities for non-work related reasons (moonlighting) and activities involving pornographic, profane, offensive, illegal or obscene content. In a survey carried out by Flowers and Rakes (2000:357), few of the AUPs reviewed included a section on netiquette (behaviour guidelines for users). These guidelines express the need for users to adhere to generally accepted rules for polite and responsible behavioural conduct on the Internet and other computer facilities.

The third area identifies the integrity and security of the Internet and intranet. Some issues outlined in AUPs reviewed by Flowers and Rakes (2000) include notification of system administration of any security problems, avoiding the demonstration of suspect activities to other users and refraining from using other users' digital identities. These are common practices that need to be emphasized to create security conscious users. Concerning the privacy for users, each policy should state that the organization reserves the right to examine and monitor individuals' usage of the Internet for the purpose of maintaining the integrity of the Internet within the organization.

The fourth area deals with the content found on Internet applications. Some policies state that the transmission of illegal material stated in present law was prohibited. The term 'illegal' should be further substantiated or explained in an AUP. Various terminologies are used to describe and define inappropriate content in material generated by the users.

6.2 Hierarchical analysis of AUPs

According to the Oxford English dictionary (2006), a hierarchy is defined as a class of items according to their relative importance. A hierarchy illustrates ranking or order of importance according to the objectives to be achieved by the task at hand. Not all objectives are equally important and therefore can be ranked in the form of a hierarchy.

Previous AUP analysis tools did not rank or order the importance of content contained in an AUP. Organizations should prioritize objectives in their AUP to ensure that they are clearly stated within the policy. By ranking objectives in the form of a hierarchy, the organization can gauge the effectiveness of an AUP.

This analysis approach was developed by identifying trends from various researches (Flowers and Rakes 2000; Kelehear 2005; Scott and Vass 1994; Simbulan 2004 and Surfcontrol 2005). Concurrently, areas of concern were identified where important concepts were missing from the consulted literature. A hierarchical structure was a natural progression as the concepts identified more often were placed higher in the hierarchy, denoting importance (Figure 1). The hierarchy consists of the following areas of analysis: legal,

security, netiquette, privacy and organization property.

Figure 1 Hierarchical analysis of AUPs

6.2.1 Legal issues

The most important point of analysis of any AUP is the legal concern and for this reason it is located at the top of the hierarchy (Figure 1). When designing an AUP, all legislation that could apply to the computer facilities and infrastructure, supplied by an organization, should be carefully considered. Most of the statements in an AUP are based on certain laws. It is important that all policies implemented are checked by law professionals specializing in the digital environment. References should be made to specific laws and acts, governing the acceptable use of the computer facilities.

Organizations need to adhere to copyright laws. Personnel and members should be informed of the seriousness of copying material available from the WWW, electronic journals and digital library resources. Issues of software licensing and unauthorized downloading of software need to be adequately addressed in this section.

This area of analysis is interconnected with the other key areas. The legal protection of an organization is the biggest overshadowing influence in the construction of an AUP.

6.2.2 Netiquette

'Netiquette' is derived by fusing the word 'network' and 'etiquette'. Netiquette refers to the etiquette of networks. Netiquette is frequently used by employers or organizations that offer employees or members access to networks outside of its own. This section of the AUP usually includes clauses on the use of content containing pornography or hate speech (Scheuermann 1997).

It is essential that an AUP has a section describing the behaviour expected from personnel and members while using the computer facilities provided, whether on the intranet, the Internet or any other online facility provided. For this reason netiquette is placed second in the hierarchy (Figure 1).

A list of do's and don'ts is usually also included in this section. The netiquette section may differ among organizations and needs to reflect the views outlined by the broad policy or

code of conduct in place. This section may address the need to respect the rights of other users on the network. Policy on changing settings and software on computer facilities provided, as well as enforcing the prohibition of using computer facilities for moonlighting activities, should also be communicated under this section.

6.2.3 Security

Computer security and security of digital resources can be defined as 'a shield that companies and governments use to protect sensitive and classified information from unauthorised use' (Forcht and Sanderson 1996:32). Issues around security need to be addressed in the AUP. The security of information is vital for any organization. Information needs to be safeguarded from any negative use or bad publicity. Security policies are necessary as sensitive data are more susceptible to attack or intrusion through an electronic medium. General security practices need to be emphasized, including the use of user accounts, password protection, policy towards hacking and implementation of anti-virus measures.

Security is crucial for ensuring the protection of information from internal and external threats. For this reason security is ranked third important in the hierarchy (Figure 1). At the same time privacy needs to be maintained by adhering to strict security regulations. Privacy and security are two seemingly conflicting aspects that need to be clearly outlined to avoid invasion of privacy. Awareness programmes should also be used as a means of updating employees on current threats and can act as a reminder to ensure adherence to the necessary precautions.

6.2.4 Privacy

Privacy is centred on the protection and ethical use of personal data. This area of policy concern must be communicated. Addressing privacy in a policy is vital for the establishment of trust (Iliadis, Moulinos and Tsoumas2004:351). The rights of users need to be respected at all times. There is a fine line between monitoring network usage and invasion of one's privacy. AUPs need to outline monitoring procedures employed as well as explain the reasons for monitoring network usage. Users' privacy rights are often undermined and little is done to protect these rights. This area of concern is often over looked in AUPs and is ranked fourth in the hierarchy (Figure 1).

6.2.5 Organization property

Lastly, AUPs need to address expected conduct tolerated with regard to the organization's property. Facilities such as computers, printers, routers, other hardware and software need to be accounted for. These facilities provided remain the property of the organization; any theft or defacing of these facilities would constitute an offence for which punishment or even legal prosecution may result. Many AUPs fail to address this area of concern, which may be considered rhetorical. Organization property is ranked fifth in the hierarchy (Figure 1).

top

7 Conclusion

AUPs play a vital role in controlling access to unacceptable content and ensuring responsible network usage. These policies set the guidelines for content and facility control, ensuring that all stakeholders are consulted. AUP analysis is important for ensuring the effectiveness of an AUP, by creating a comprehensive policy to guide users on how to use the facilities provided. AUP analysis should be an ongoing task as the nature of the online environment is evolutionary and forever changing.

The hierarchical analysis of an AUP, consisting of the sections legal issues, netiquette, security, privacy and organizational property, allows for a structured and ordered way of organizing an AUP. It is an effective tool for highlighting the important areas of concern. It is impossible to include every necessary policy stance in a workable AUP and this should be kept in mind when analysing an AUP. Through this structured approach, an assessment of an AUP becomes effortless.

top

8 References

Chen, J. Chen, C.C. and Yang, H. 2008. An empirical evaluation of key factors contributing to Internet abuse in the work place. *Industrial Management and Data Systems* 108(1):87-106.

Forcht, K. And Sanderson, E. 1996. Information security in business environments. *Information Management and Computer Security* 4(1):32-37.

Flowers, B. and Rakes, G. 2000. Analyses of acceptable use policies regarding the Internet in selected K-12 schools. *Journal of Research on Computing in Education* 32(3):351-365.

Held, G. 1999. Beware of a new potential liability. *International Journal of Network Management* 9(1).

Hughes, J. 2004. Ten tips for implementing an acceptable internet use policy. [Online]. Available WWW: http://www.computerworld.com/printthis/2004/0,4814,94231,00.html (Accessed 13 March 2009).

Iliadis, J. Moulinos, K. and Tsoumas, V. 2004. Towards secure sealing of privacy policy. *Information Management and Computer Security* 12(4):350-361.

Kelehear, Z. 2005. When Email goes bad: be sure that your AUP cover staff as well as students. *American School Board Journal* January: 32-34.

Kinnaman, D. 1995. Critiquing acceptable use policy. [Online]. Available WWW: http://www.io.com/~kinnaman/aupessay.html (Accessed 13 March 2009).

Kleiner, B. and Welebir, B. 2005. How to write a proper internet usage policy. *Management Research News* 28 (2/3).

Lichtenstein, S. and Swartman P. 1997. Internet acceptable use policy for organisations. *Information Management and Computer Security* 5(5):182-190.

Net Dictionary. 2004. Acceptable use policy. [Online]. Available WWW: http://www.netdictionary.com/a.html (Accessed 13 March 2009).
Oxford English Dictionary. 2006. Oxford. Oxford University Press.

Scheuermann, L. and Taylor, G. 1997. Netiquette. *Internet Research: Electronic Networking Applications and Policy* 7(4):269-273.

Scott, V. and Voss, R. Ethics and the 7 'P's of computing use policies. *Ethics in Computing Age*: 61-67.

Seymour, L. and Nadasen, K. 2007. Web access for IT staff: a developing world perspective

on Web abuse. *The Electronic Library* 25(5): 543-557.

Simbulan, M. 2004. Internet access practice and employee attitudes towards Internet usage implementation in selected Philippines financial institutions. *Gadjah Mada International Journal of Business* 6(2): 193-224.

Splitt, D. 2001. Backup your filtering with an airtight AUP. [Online]. Available WWW: http://www.eschoolnews.com/news/showstory.cfm?ArticleID=2755 (Accessed 13 March 2009).

Stott, D. 2001. Your Internet acceptable use policy. *PC Support Advisor*. August 7-10.

Surfcontrol. 2005. How to write an acceptable use policy (AUP). [Online]. Available WWW: www.surfcontrol.com/uploadedfiles/**AUP**_Booklet_10011_uk.pdf (Accessed 13 March 2009).

Wikipedia. 2005. Acceptable use policy. [Online]. Available WWW: http://en.wikipedia.org/wiki/Acceptable_use_policy (Accessed 13 March 2009).

ISSN 1560-683X
Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg