



# Creating and Managing Effective Acceptable Use Policies

## ABSTRACT

This short paper is intended for IT decision makers, HR managers and executives responsible for adopting and enforcing email and Web Acceptable Use Policies (AUPs) within an organization. It aims to identify some of the complexities involved in creating and managing an AUP and demonstrate that a successful AUP is more than a simple list of dos and don'ts.

## INTRODUCTION: WHAT IS AN ACCEPTABLE USE POLICY?

Nearly all organizations now rely upon information technology to do business. Most office-based employees have access to a computer and many have a laptop or PC that is dedicated to their business use but also for their own personal use. Both email and the Internet provide employees with essential tools that enable them to do their jobs. However, technology is also open to abuse.

For many years employers have issued guidelines to their staff relating to the acceptable use of telephones at work. Most companies usually adopt a pragmatic approach and permit reasonable personal use of their telephones, excluding, for example, lengthy or international calls. Others have been more draconian and issued a clear edict that no personal use is permitted whatsoever. With the increased importance and use of email and Web at the workplace, these guidelines are frequently extended to include all areas of information technology, eventually becoming what is commonly called an Acceptable Use Policy (AUP).

## DO YOU REALLY NEED AN ACCEPTABLE USE POLICY?

AUPs have become far more important than simply ensuring a user isn't spending their whole working day surfing the Web, exchanging jokes and pictures or chatting with their friends or family. The reliance upon IT and the nature of the data that passes through it is often fundamental to the successful and smooth running of a business or organization. Any compromise or failure of the system has the potential to be catastrophic and can result in anything ranging from the merely irritating or mildly embarrassing to criminal prosecution and a prison sentence for corporate officers.

While an IT team can manage and control the hardware and software across their network, they have a much more difficult job with the end-users, who are often considered to be the weak point in an otherwise secure network.

Indeed, when criminal organizations launch campaigns to augment their botnets, infiltrate organizations or obtain sensitive or personal data, they actively target end-users. By employing "social engineering" techniques to entice unsuspecting users to open a malicious email attachment or visit a website that will attempt to exploit any unpatched vulnerabilities in their web browser, the criminal gangs are attacking the soft underbelly of the network. Increasingly common is the use of seemingly innocent emails containing links to websites hosting malicious code, commonly known as blended threats. For detailed examples of these techniques, visit the M86 Security Labs blog at <http://www.m86security.com/trace/traceblog.asp>

An effective AUP, especially when used as the basis for an IT Security training programme for all members of staff, can help ensure productivity while increasing security at the same time. As such, a good AUP can be seen by both employers and employees as a positive (rather than restrictive) measure. It's guideline that enables use of Information Technology for everybody but without the risks.

## CREATING AND DEVELOPING AN AUP

The content of an AUP will undoubtedly vary between organizations. There are many examples of suggested starting points for those that are responsible for writing an AUP available on the Internet. Some good, independent sites providing this information include:

- Business Link: [www.businesslink.gov.uk](http://www.businesslink.gov.uk)
- ICTKnowledgebase: [www.ictknowledgebase.org.uk/acceptableusepolicy](http://www.ictknowledgebase.org.uk/acceptableusepolicy)
- Becta: [www.becta.org.uk](http://www.becta.org.uk)

The M86 white paper entitled "Inbound and Outbound Content Security" also suggests seven checklist points that can form the basis of an AUP:

- Allow limited personal use of Web and email
- Outline what is acceptable and what is not; while preserving company culture
- Be consistent with enforcement and setting precedents
- All email should be identified with a name or email address – avoid spoofing
- Copyright - inform staff on copyright issues relating to email or Internet documents
- Monitoring and enforcement - inform staff about what is acceptable inside business hours and what is acceptable outside of business hours, if there is any difference. This needs to be clearly stated in the policy.
- Reserve the right to monitor all messages/files on the company network

Regardless of content, however, to be really successful and Acceptable Use Policy must meet the following criteria and be:

**1. Adaptable.** Many organizations have some sort of AUP written into the terms and conditions of their employment contracts or an associated document. Unfortunately, these tend to be static, non-specific and almost invisible to the end-users with fewer than half (45%) of organizations updating or changing their AUP over the last twelve months\*. The Internet has changed dramatically over the last five years and will continue to do so. To be effective, an organization must be willing to review its AUP in order to adapt and address emerging threats, new regulations and changes in use of email and the Internet. A good example of this is You Tube. For several years, You Tube was considered to be a waste of time as far as businesses were concerned. They didn't want employees to watch funny clips or music videos all day long. Increasingly, however, many organizations have started to see the benefits of sites like You Tube. Some now use these sites for training purposes as well as for sales and marketing; thus making the site available to their staff, but amending their AUPs to ensure its usage is not abused.

**2. Flexible.** Any AUP must be flexible enough to meet the requirements of the organization for which it is written. A 'one-size-fits-all' approach is rarely sufficient and will either be too restrictive for employees to do their work or too open to abuse. Different departments may well have very different notions of sites that are deemed suitable; they may also work different hours or have different responsibilities. Two examples from the Public Sector are Local Authorities and Hospitals. Most Local Authorities have Social Services departments who often need access to harrowing, upsetting and potentially offensive material and images. Employees working in this area will therefore need to be exempt from some areas of the AUP. Likewise, many hospitals have members of staff who live on-site. While an Acceptable Use Policy might restrict them from visiting certain websites during working hours, it is unlikely that the hospital or trust will want to enforce these rules during an employee's time off.

**3. Enforceable.** To be successful, an AUP must be enforceable. This usually requires the installation of security software or hardware that is able to monitor, block and report on any unacceptable use of an organization's IT infrastructure. In a survey conducted by M86 Security, a quarter (25%) of respondents said that their Internet and email acceptable use policy was not actively enforced and over a third (38%) stated that they relied upon managerial vigilance alone to enforce the AUP. The policy should also be enforced in a fair manner, encouraging users to admit mistakes rather than try and cover up something that may have wider implications. Likewise, senior members of staff should not be exempt from the policy. Additionally, the ability to generate detailed reports based upon individual or group activity over a prolonged period of time is vital to enforcing a policy properly.

**4. Visible.** Employees should be reminded of the AUP and some of the implications of breaking it. Policy breaches, accidental or otherwise, should result in a notification (via email or Web page) to the user telling them what they did, why it was wrong and reminding them that they are being monitored.

With increased Web usage in the workplace, it is also a good idea to have a regular reminder displayed in the browser where the user has to acknowledge acceptance of the corporate AUP on a daily, weekly or monthly basis before continuing. Training and educating staff about IT security will also help with visibility and ensure that users understand that the AUP is there as much to protect them from phishing attacks, obscenity and abuse as it is about controlling what they do during working hours as well as protect the organization's infrastructure.

**5. Supported.** An AUP is not the responsibility of the IT department alone and the IT team should not be expected to police email and Web usage. Although IT are usually responsible for installing and managing security technology, as well as running reports on users or groups of users as required, the overall responsibility should lie with the entire management team and HR to ensure all departmental requirements are met. Additionally, IT security and any associated policy should be supported at a senior executive level. Board level support will ensure that the AUP is taken seriously and that the threats posed by email and internet usage are understood properly. Without senior support, an AUP runs the risk of becoming a set of toothless guidelines.

## CONCLUSION: MEETING THE REQUIREMENTS

With 40% of organizations reporting that they have had to discipline members of staff over the last 12 months because of breaches of their corporate AUPs\*, it is clear how important it is to establish and manage a policy. While managerial vigilance can be effective at enforcing an AUP in very small offices, it is no replacement for security tools that have been written to perform precisely this task.

Organizations should look for solutions that help them meet the requirements mentioned above.

- Using products that integrate with LDAP or Active Directory will enable an organization to create flexible policies based upon group membership.
- Using a solution that can apply rules to users on a scheduled basis, such as during working hours, will add to this flexibility.
- Regular scheduled reports mean that managers can get on with their jobs instead of policing their staff, while alerts and notifications can provide instant information about potential threats and help train users in safe computing techniques by letting them know what they have done and why it was not permitted.

As well as providing tools for managing an AUP, security products give essential protection against the ever-present Web and email threats. No matter how well a policy is constructed, it is inevitable that at some point it will be breached and will need enforcing. Identifying content within email and Web traffic and blocking it as appropriate is an essential part of an organization's overall infrastructure. As a result this will help protect against malware, prevent data leakage, copyright theft, manage inappropriate material and achieve regulatory compliance.

## M86 SOLUTIONS FOR ENFORCING AUPs

### Email Security

**M86 MailMarshal Email Content Manager (ECM)** - one of the few solutions available in the market to provide email management that filters and manages internal inbox-to-inbox email for organizations. It monitors and controls internal email content that travels within an organization to ensure a safe, productive working environment and compliance with acceptable use policies.

**M86 MailMarshal Secure Email Gateway (SEG)** - an email security solution that combines email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible, easy-to-manage solution. MailMarshal SEG acts as an email gateway, powered by an unrivalled Defense-in-Depth Anti-Spam Engine, which filters all incoming and outgoing email at the network perimeter.

**M86 MailMarshal Secure Email Server** - a dedicated policy-based secure email solution that provides encryption, digital signing and deep content inspection of inbound and outbound email messages. It operates with any email gateway that can recognize S/Mime encrypted email, and automatically updates contact details and secure certificate credentials for encryption contact via a centralized server.

**M86 MailMarshal Managed Services Platform (MSP)** - a SaaS security solution which enables Managed Service Providers and Internet Service Providers to offer hosted email content security services to any size of school or small office/home office (SOHO) customers. It combines email filtering, anti-spam, anti-virus, anti-pornography, anti-phishing, policy compliance, email archiving and reporting into a centrally managed, highly scalable architecture.

### Web Security

**M86 Web Filtering and Reporting Suite** - helps organizations enforce AUPs and comply with regulations easily. Known for its fast performance and multi-tiered administration capabilities, the M86 WFR sits outside the flow of network traffic to quickly and accurately filter millions of websites in 100+ categories—without impacting bandwidth or productivity.

**M86 WebMarshal** - the most complete secure Web gateway solution on the market today. It goes beyond URL filtering to provide comprehensive Web access control and management, complete threat protection (URL, AV and malware filtering) and data leakage prevention in a single, policy-based, easy-to-manage and highly scalable solution.

## REFERENCES

1. M86 Acceptable Usage Policy survey, November 2008: Question 7. When asked if their acceptable use policy had changed in the last twelve months, 75 out of 128 respondents said that it hadn't.
2. M86 Acceptable Usage Policy survey, November 2008: Question 3. When asked how their organization enforced its internet and email acceptable use policy 34 out of 136 respondents said that it was not enforced and 51 out of 136 respondents indicated that it was enforced by managerial vigilance.
3. M86 Acceptable Usage Policy survey, November 2008: Question 6. When asked if any employees at their organization had faced disciplinary action in the last twelve months, 51 out of 128 respondents said that they had.

## ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: [www.m86security.com](http://www.m86security.com).

## TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Corporate Headquarters**  
8845 Irvine Center Drive  
Irvine, CA 92618  
United States

Phone: +1 (949) 932-1000  
Fax: +1 (949) 932-1086

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom  
Phone: +44 (0) 1256 848 080  
Fax: +44 (0) 1256 848 060

**Asia-Pacific**  
Suite 3, Level 7, 100 Walker St.  
North Sydney NSW 2060  
Australia

Phone: +61 (0)2 9466 5800  
Fax: +61 (0)2 9466 5899

Version 04/15/11