

Effective IT Policies

Acceptable Use Policy and the threat of lifestyle devices

The role of an Acceptable Use Policy (AUP)

Today, businesses critically depend on IT systems and the data they have cultivated in order to communicate with staff, customers and partners; to trade effectively; to manage complex relationships and to monitor operational performance. This increased dependence upon IT raises a number of juxtapositions around security and availability that corporations need to navigate effectively in a changing IT environment. For example:

- The need for availability of essential data for operations balanced with the need for confidentiality
 - The need to protect the company and its customers data balanced with the need to protect the rights of employees
 - The need to protect the company from threats arising outside the company AND the threats arising from inside the company
 - The need to demonstrate regulatory and statutory compliance for data protection and confidentiality, balanced with the need to use information seamlessly in the delivery of services
- The need to embrace or support the role of lifestyle computing (internet, PDAs etc) upon employees whilst keeping the corporate network clear of any personal computing liabilities
 - The classic view of Corporate IT networks and systems and how that is impacted by the increasing trend toward remote and mobile workforces

At a time when the relationship between employees and information technology has never been more essential, companies need to navigate their path carefully to avoid the manifold pitfalls – but navigate the path they must – as inaction, like ignorance, is not a defence to the issues they face if they leave the matter unresolved.

The AUP is a critical component in the education of employees to IT risks and the benchmark for enforcement and discipline inside the company. It must be capable of enforcement to carry any credibility.

A layered approach to security and availability

The philosophy that 'one size fits all' never proved to be true in the clothing industry and is equally untrue when considering the policy organizations put in place to govern employee interaction with corporate IT systems and data. However, organizations can make dramatic improvements in the effectiveness of their IT security if they follow some simple steps to quantify risk and focus their attention on the key issues. We would summarize these steps as:

- I. Understand your acceptable risk
- II. Fix the big holes first
- III. Avoid unnecessary complexity
- IV. Step back - does your policy pass the 'Common Sense' test?

One of the single biggest security impacts upon corporate IT is the encroachment of lifestyle computing devices (e.g. phones, PDAs, mp3 players and USB storage gadgets) in the workplace. Whether the intent is good or ill, these devices bypass traditional security measures and provide a high volume, high speed and low cost portable file store to interact with the network via a USB or Firewire port. Uncontrolled, these devices can introduce inappropriate material to the corporate network or discretely remove your company's sensitive data. This is a classic area where policy alone, without the ability to enforce it, is nothing more than a modern metaphor for the story of King Canut who foolishly demanded that the tides should obey his rule.

I. Understand your acceptable risk

It is not difficult to comprehend the threat of uncontrolled removable media devices to a business, but in tackling the issue you equally need to understand the legitimate use cases that may exist for this technology and, indeed, the prevalence of such devices already operating within your business.

To implement an effective AUP, you will need to determine the impact of it upon the organization from both an education and enforcement perspective. Therefore you will need visibility of what devices are connecting to the network, by whom, for what purpose, and finally if there is a better way to achieve the task.

By understanding this information you de-risk the possibility of accidentally blocking legitimate use, incurring unnecessary overheads in managing the fall-out of suddenly blocking previously unblocked devices, and you ensure the goodwill of employees in the roll out and acceptance of the policy.

Locking down USB ports entirely is not a viable solution as employees need access to them to connect a mouse, keyboard or printer for example, or to enable legitimate plug

and play devices being used for corporate approved services (such as a file transfer by a Help Desk engineer or a diary synchronization by a field sales person).

In determining your company's acceptable risk you should also be prepared to tackle the obvious issue that if a removable media device is required to be used – it should therefore be supplied by, and owned by, the company and not an individual employee. This formal separation is an important test in determining the ownership and usage of the information contained on it as well as of the device itself.

So – what is your level of acceptable risk? One uncontrolled connection, 100 uncontrolled connections, or more? What are the odds that any single instance that is uncontrolled (and therefore unmitigated) could be the loss of your customer details, product designs or credit card transaction details? What would the consequences of that breach be to your business – only your business can decide that – but once decided, you need an enforceable policy to mitigate the risk.

II. Fix the big holes first

Many people when implementing policy aim to be too granular in its design too quickly. In implementing an effective AUP you are seeking to limit the risk to your organization from inappropriate employee activity. In order to achieve this goal whilst not disenchanting your employees, Centennial advocates a layered approach to implementing policy by assessing the risk and closing off the big holes first; then monitoring operational impact of the policy; reviewing the policy as necessary, and then moving to the next stage of implementation – and so the cycle continues.

While the vast majority of activities that might be considered inappropriate are usually not malicious in their intention (copying files for business use, synchronizing PDAs etc.), the fact is that in an 'uncontrolled' environment the risk of an inadvertent security breach is simply too high. This is because the company cannot rely on a security policy that is based solely on user co-operation and understanding. We are all human and therefore are prone to making mistakes - intentional or otherwise!

So in implementing a policy a company should close off the biggest holes first to protect their business from the most obvious threats by likelihood or severity of impact.

For example, with very few legitimate exceptions, employees should not need to connect either an iPod or a camera to the corporate network.

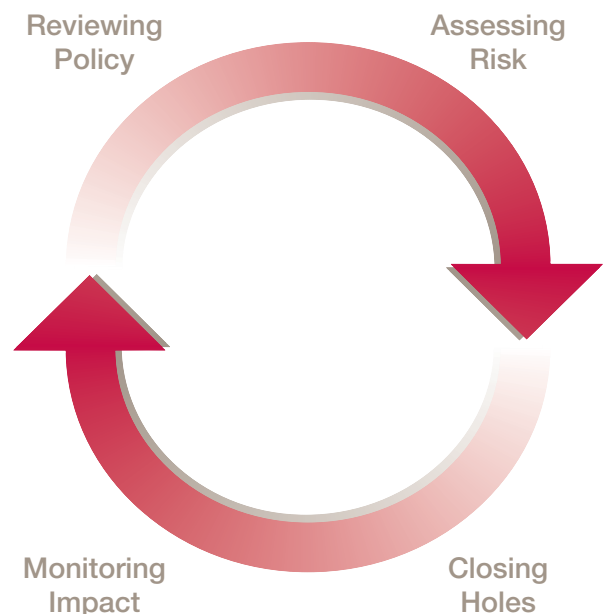


Fig 1.0 – The policy management cycle

Therefore, you should be able to block en-mass the use of these devices by employees.

Equally, the use of USB storage devices should not be used for the ad-hoc or planned data movements other than by specifically exempted staff.

Finally most companies will be happy to allow CDs to be read but not written to.

So, very quickly and simply it is possible to set up a policy that meets the bulk of the operational risk facing a business. However, one size certainly does not fit all, and therefore policies will inevitably evolve over time as the uncontrolled activities become more visible and the needs of the business emerge.

Using DeviceWall customers gain a number of unique advantages in setting and managing effective policies which fundamentally reduce the total cost of operation and enforcement of the AUP, such as:

1. DeviceWall allows you to run an audit of network activity over a timeframe of your choosing so that you can monitor who is using what devices, where and when. This enables you to assess legitimate use cases that may otherwise have remained invisible, as well as highlighting the scale of uncontrolled use in the business.
2. DeviceWall enables you to grant temporary access to a user for specific device types, enabling users normally covered under the baseline policy to be granted managed and audited exceptions for specific purposes.
3. DeviceWall enables you to inform users proactively of the policy operating in the business whenever they log onto a machine and can alert them if they attempt to use a

prohibited device. As the messaging is configurable you can avoid wasted administrative effort in handling people's concerns about policy in force by directing them on how and when they might be granted access.

4. DeviceWall agents proactively look for the latest updates in policy to ensure that they are managing the user interface in accordance with the currently prevailing policy. There is no need for manual intervention to push out policy to protected machines.

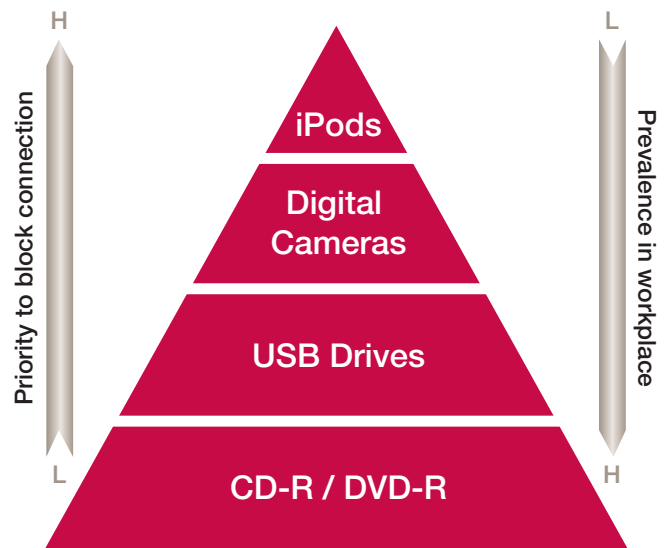


Fig 2.0 – Building a layered approach

III. Avoid unnecessary complexity

For security to be effective it needs to avoid ambiguity, be reliable and mitigate the obvious threats. At the end of the day there is a trade off between granularity of policy against the cost of execution and management. Businesses often overlook the inherent weaknesses involved in managing too fine grained a policy before they have really begun to manage and mitigate the real risks. This can result in the failure of the policy, or excessive costs in managing the policy or both. Common areas of weaknesses companies fail to navigate include:

- Offering different policies by machine, rather than enforcing the rights of a person regardless of the machine used
- Offering variations to policies at varying times of day; as if the risk were more real at certain times of day than others!
- Trying to manage named or identified devices in the corporation that may be used at the expense of all others, without resolving the issues around access to these devices and the management of them throughout their lifecycle
- Having to manually manage the status of the policy deployed on to PCs and push new policy updates, rather than having an automated process that pulls down the latest policy whenever an asset connects to the network

- Failing to effectively tie the employee awareness of policy to the experience of trying to use a device, wasting time in support operations

DeviceWall has been designed to offer the easiest determination, implementation and enforcement of policy, giving you complete visibility and control of your IT estate and the interaction of Plug'n'Play devices.

IV. Does your policy pass the 'Common Sense' test?

An AUP by nature is defined to influence employee behaviour and therefore be enforced in the manner it is written. This requires the solution to be intuitive in terms of business rules, referenceable and understandable to users, and intelligent in its management, change control and enforcement.

DeviceWall offers the most cost effective solution for complete enforcement of an AUP. Quality technology, designed with business reality in mind provides a solution with the least cost of ownership over its operational life.

Turning words into action: A draft Acceptable Use Policy

The sample policy below has been drafted with the assistance of specialist IT and employment law firm, Cater Leydon Millard. Certain areas of this policy, which are especially important when considering the threat of portable devices, have been colour-coded in red.

While this draft document is designed to help you understand how your computer use policies need to address the various

risks facing your organization, it is not intended to be definitive statement. Legal advice should always be sought before taking action in reliance on any information contained in this guide or in the preparation of a policy governing the use of an organization's IT network.

Draft Policy

Introduction and Scope

1. This Policy relates to the use and monitoring of all of the Company's IT and communication systems, including telephones, mobile telephones, facsimile machines, computers (including laptops and personal organisers), email, the internet, the intranet and the extranet.
2. The Company provides the IT and communication systems for business purposes and the use of these systems at all times is subject to this policy. Breach of this Policy in your use of the Company's IT and communication systems will be considered a disciplinary issue.
3. This Policy applies to all employees, contractors and agents ("staff") who use the Company's IT and communication systems.

Email

4. Email correspondence is not private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. You must take into account the fact that any email you send may be read by a person other than your intended recipient.
5. Any attachments which contain important or confidential material should be encrypted or password protected.
6. All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of protection. All employees have an obligation to be cautious when opening emails and attachments to emails from unknown sources. If you have any doubts about opening an email or attachment, speak to the IT Department first.

7. Contracts can be entered into by email in the same way as they are by letter or on the telephone. You must at all times take care to ensure that you do not inadvertently enter into contracts which bind the Company by email, and you should be aware that contracts must only be entered into in accordance with the normal procedures.
8. You must not under any circumstances send messages or attachments whether within the Company or outside the Company which are:
 - a. Abusive including the use of foul language
 - b. Malicious
 - c. Discriminatory in any sense (e.g. sex, sexual orientation, age, race, religion, gender or disability)
 - d. Defamatory about any other person or organisation
 - e. Bullying or intimidating in content
 - f. Sensitive or confidential

If you receive any such messages from outside the Company you must delete them and must not forward them either within or outside the company.

Sending emails of the type described above is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct.

Internet

9. The Company has put technical measures in place to prevent access to internet web sites which contain explicit, illegal or other inappropriate materials. If you need to access a site which contains such materials for the purposes of your job you must obtain the express permission of the Company.
10. Much of the information that appears on the internet is protected by copyright. Unauthorised copying or modifying of copyright protected material, including software, breaches copyright law. Therefore, downloading software or copyright protected information is not permitted, as it may make you and/or the Company liable to legal action.

Confidentiality

11. You must not use the Company's IT and communications systems whether alone or in conjunction with any other device to make an unauthorized disclosure or copy of confidential information belonging to the Company.
12. The unauthorized disclosure or copying of information belonging to the Company is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct
13. Such confidential information shall include without limitation details of:-
 - a. Business contacts, associates, lists of customers and suppliers and details of contracts with them
 - b. Identities of potential customers and suppliers
 - c. Sales, expenditure levels and buying and pricing policies including details of percentage mark-up of profit and discounts
 - d. Proposals, plans or specifications for the development of the existing products and of new products to be sold or developed
 - e. Accounts, trading statements, statistical information and other financial reports
 - f. Corporate and marketing strategy, business development plans, sales reports and research results and forecasts
 - g. Details of the employees and officers of the Company and of the remuneration and other benefits paid to them
 - h. Presentations, tenders, projects, joint ventures or acquisitions and developments contemplated, offered or undertaken by the Company

Monitoring and Data Protection

14. In order to protect the interests of the Company and to maintain the effectiveness, integrity and security of the Company's network, the Company has tools in place to monitor and intercept telephone and email communication and internet use by staff.

15. Monitoring is undertaken using the following automatic procedures:
 - a. Automatic checking of emails and attachments for viruses.
 - b. Automatic checking of emails for multimedia attachments and offensive words.
 - c. Automatic checking of disks, CDs and internet sites for viruses
 - d. Automatic measures in place to prevent software from being downloaded to, installed on or deleted from the Company's computers
 - e. Automatic blocking and recording access to certain files and pages on the internet
 - f. Automatic recording of telephone and mobile telephone call destination numbers
 - g. Automatic blocking of access to premium rate telephone lines
 - h. Automatic blocking of the connection of unauthorised devices to the network
 16. Monitoring of the content of emails, internet use or telephone calls is not routinely carried out but may be carried out in some situations. For example (this is not an exhaustive list):
 - a. Where the Company has reasonable grounds to believe a staff member is breaching this or any other policy of the Company
 - b. Where there is a suspected breach of contract or a serious under-performance
 - c. For the purpose of assisting in the investigation of wrongful acts
 - d. To comply with any legal obligations
 - e. For the purpose of defending or prosecuting any legal action brought against the Company
 17. You should not expect that your personal use of the Company's IT and communication systems to remain private.
 18. The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of data protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent by mail unless proper checks have been made to ensure that this will not involve any breach of that legislation.
 19. You must also comply with the Company's Protection Policy.
- Security**
20. Employee access to the Company's IT and communication systems is subject to satisfactory security checks being carried out in the reasonable discretion of the Company.
 21. **If you are provided with a portable computer, mobile phone, personal organiser and/or any related or similar equipment, you must ensure its security at all times. You must in particular**
 - a. **Never leave computer equipment including discs, CDs and DVDs in an unattended vehicle, or unattended in public**
 - b. **Always lock mobile equipment when not in use so that it cannot be used without entering your log-on ID**
 - c. **Keep your passwords confidential and the IT system will force you to change them regularly**
 - d. **Lock the terminal if you leave a terminal unattended so that it cannot be used without entering your log-on ID in order to prevent unauthorised users using it in your absence**
 22. If your computer equipment is lost or stolen you must report the incident to the police immediately, and notify your line manager as soon as possible. The incident will be fully investigated, and may be treated as a disciplinary issue if you have failed to take adequate steps to safeguard the security of equipment in your possession.
 23. You must not attempt to gain access to any part of the network to which you are not permitted access.

Computer and other equipment not provided by the Company

24. You must not connect or attempt to connect any device to the network without express authority from the IT Department and you should be aware that the Company has in place automatic measures to prevent this.
25. In particular you should not attempt to connect any of the following devices to the Company's network:
 - a. An unauthorised file or information storage device
 - b. A mobile phone or PDA not issued by the Company
 - c. An MP3 Player or similar device
 - d. A gaming device
 - e. A camera or flash memory card
26. A breach of the prohibition contained on connecting devices to the Company's network is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct.

Personal Use

27. A limited amount of personal use of the Company's systems is permitted subject to the following rules:
 - a. Work on the Company's business must always take priority over your personal use of the Company's systems
 - b. Any personal use must not delay or interfere with the proper performance of the duties of any member of staff
 - c. All personal email messages must make it clear that they are sent in a personal capacity and not on behalf of the Company and must include in the subject field a statement that the email is "Private"
 - d. Where you are in receipt of personal emails you should advise the sender that these may be monitored
 - e. All personal emails should be deleted as soon as read or sent
 - f. You may not subscribe to any non-job related Internet service or access any web based personal email accounts using the Company's systems

- g. You may not use the Company's systems to transfer, store or download information and files for your personal use including (but not limited to) MP3, AVI, WMV files and other similar formats

If your personal use exceeds an acceptable level in the reasonable opinion of the Company or you do not comply with these rules your access to the system may be curtailed and you may be subject to disciplinary action.

Consequences of a Breach of this Policy

28. Breach of this Policy in your use of the Company's IT and communication systems will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:
 - a. Excessive visiting of non-job related internet sites during your normal working day
 - b. Introducing a virus to the computer system by inserting a disk, CD or DVD into a Company computer without running a virus check, via email or from downloading an Internet file
 - c. Misuse of the computer system which results in any claim being made against the Company
 - d. Accessing pornography or any other illegal material on the Internet and/or circulating it
 - e. **Unauthorized copying or modifying of copyright material**
 - f. Unauthorized downloading of software or files
 - g. **The connection of an unauthorized device to the network**
 - h. Use of the Internet for criminal activity

In less serious cases you may have access to the internet from your computer removed or other disciplinary action taken against you short of dismissal.

End of policy