2
Policy

This is a story about Havensburg University, which doesn't exist. The elements of its story are taken from those of many different institutions and organisations, and are assembled to illustrate the scope and limits of policy in managing bandwidth.

Havensburg first connected to the Internet in 1988, with a circuit initially of 64 kbps, rising to 192 kbps by 1992. During these years the dominant protocols on the Internet were email, ftp, gopher, and nntp. Users were mostly in the scientific community, and they generally used one of three shared Sun computers. Almost every member of the Internet user community on the campus knew every other.

In 1992, things had started to change. Ethernet networks had started to become common on the campus. With some difficulty, users of these networks could get a TCP/IP stack on their PC and a connection to the Internet. Email had come into increasing use in the non-scientific community. Windows 3.0 began to appear on PCs. Its graphical user interface made the PC attractive to non-technical users. In 1993 the NCSA Mosaic browser was released; later that year, the first commercial websites appeared. By 1994 the web was clearly the dominant Internet service. Havensburg's academic community clamoured for access to it; in response, the University approved plans for increased expenditure on the campus network, and doubled the capacity of the Internet connection to 512 kbps.

By 1996, enterprising academics were demanding Internet access for students, and the first large student computer labs began to appear. In the space of two years, the number of hosts connecting to the Internet had risen **tenfold**. Despite the increase in bandwidth, response times had fallen dramatically. Academics were starting to complain aggressively about poor performance, and the University Budget Committee had started to balk at the cost of Internet access. Despite this, the build-out of student computer laboratories continued, and many academic departments were insisting on a PC for every member of staff. Non-academic departments were beginning to demand the same.

The importance of policy

An abundance of bandwidth enables electronic collaboration, access to informational resources, rapid and effective communication, and grants membership to a global community. An absence of bandwidth prevents access to the aforementioned global community, restricts communications, and slows the speed at which information travels across the network. Therefore, bandwidth is probably the single most critical resource at the disposal of a modern organisation.

Because bandwidth is a valuable and costly resource, demand usually exceeds supply. In many environments, unrestrained access and usage of bandwidth results in degraded service for all users. This is partly a supply problem (not enough bandwidth is available to meet demand), partly a demand problem (too many demands are being made on the limited resource), and partly a technical problem (little or no technical management and optimisation of the resource is happening). The end result is a poor user experience when trying to use resources and tools that rely on bandwidth (e.g., browsing the web, sending emails, using network applications, etc.).

Bandwidth management and optimisation are often seen as technical issues. However, policy is an essential component of any bandwidth management strategy. Without it, technical solutions will be difficult to implement and much less effective. Policies are essential, in that they provide the framework for defining how a network is to be used and detail how technical solutions should be implemented.

Policy should be thought of as guidelines concerning network usage for both the users and those responsible for maintaining the network itself. In the case of Havensburg University, these guidelines were not developed to match the growth of the network. Without a plan, unrestricted access to the campus network would push its management into total chaos.

Explosive network growth at Havensburg

By early 1997, demand for Internet access had far outstripped supply and the Internet was effectively unusable on campus. The Computer Services Management Committee then stepped in and appointed a task team to analyse the problem and make recommendations. The team recommended doubling the available bandwidth, implementing NNTP and web caching, and aggressive pruning of the Usenet groups carried by the University's news server.

With some difficulty, the University Budget Committee was persuaded to approve the increase in bandwidth, believing that the new measures would bring an improvement in service. There was indeed a brief improvement, but by 1999 demand was again rising sharply, and the emergence of peer-to-peer networks - beginning with Napster in that year - was threatening a crisis. Academics were demanding a tenfold increase in bandwidth and were threatening to install independent connections to the Internet. Many began to use dial-up connections from their offices rather than tolerate the abysmal performance of the campus network. It became obvious that unrestricted network access could simply no longer be supported.

Bandwidth as a public good

In many institutions, bandwidth can be thought of as a ***public good***. By “public goods,” economists generally mean a resource that can be consumed by an individual in arbitrarily large amounts, irrespective of the contribution made by that individual to conserving or renewing that resource. (The technical definition is a good deal more complex, but this is sufficient for our purposes.) Public goods are notorious for being liable to over consumption, and it can be shown that the rational, self-interested individual will almost always choose to over consume – even though this leads to a collective outcome that is bad for everyone. A "public goods problem" is any problem that arises out of this paradoxical tendency. Public goods problems can be managed in a number of ways: for example, by rationing the good, by converting it from a public good into a private good, by coercing appropriate behaviour, by educating consumers, and by fostering community spirit.

Those concerned with managing bandwidth need to be informed of this dimension regarding public goods. In particular, they should be made aware that it only requires a small group of abusers to wreck the availability of 'the good' (or bandwidth) for the group at large. It is almost always the case that a small minority of (ab)users account for most of the consumption of an over consumed public good. Thus, **5-10% of users create 50-60% of the problems**.

Policy aims to manage the behaviour of this minority. If a majority are over-consuming bandwidth, then the problem is probably of a different kind: most likely of undersupply (i.e., not enough of the bandwidth is being provided to meet the reasonable needs of the users).

Good policy also has an ***enabling purpose***. Policy is not just a set of arbitrary restrictions about how a network may or may not be used. Its central purpose is to govern usage of a resource to provide equitable access to all of its users. By enacting policy, we limit the ability of the minority abusing the network to infringe on the majority who need to use the network.

At Havensburg, students were not aware of the criteria that constituted acceptable use, because no relevant policy was in place. IT staff could not solve network congestion issues because they were unable to decide which services deserved priority, and which should be cut off altogether. If Havensburg was going to continue to offer network services to faculty and students, something had to change.

Desperate measures

At this point, the Computer Services Management Committee decided to begin charging students for web access. The proposal was strongly resisted by students, who marched on the Computer Services Building in protest. Despite this, student charges for web access were eventually implemented in 2001, based on volumes of traffic downloaded. Surprisingly, this had very little effect on consumption. Some cash was generated, but university policy prevented it from being used to improve Internet access.

The Computer Services Management Committee then proposed to extend charging to staff, a proposal that was rejected by the University Executive. Instead, the Executive demanded an accounting of what the Internet access circuit was being used for, and by whom. Such an analysis had never been undertaken before, on the grounds that it would violate rights of privacy. A group of academics raised a formal protest in the University senate on precisely these grounds, but the senate finally decided that Internet access was a common good and that the rights of the community trumped the individual's right to privacy.

The University's lawyers advised that there was no inherent right of privacy when using a resource paid for by the University, provided that the University advised its members of this in advance. On this basis, the University took two decisions: first, that all users of the Internet would henceforth be authenticated, and second, that Internet usage would be analysed after a period of three months.

These announcements by themselves produced a drop in traffic, but not enough to make a major difference. After three months, log files were exhaustively analysed. The conclusions were, among other things, that:

- Not all accesses were being authenticated. Some users could not be identified by name because they were finding ways to circumvent the authentication.
- Even when users were being authenticated, the nature of their usage could not always be determined: inspection of both packet contents and source revealed no meaningful information, since the data was often tunneled and encrypted.

- A great deal of material that could be identified had no demonstrable relationship to the University's ordinary business.
- A small minority of users accounted for most of the traffic.

The IT department investigated the first issue and adopted measures to ensure strict authentication on all accesses. In the case of issues 2 and 3, attempts were made to interview users about their pattern of access. In case 2, most of the traffic was eventually identified as peer-to-peer file sharing. In case 3, responses from users were mixed. Some denied all knowledge of having generated the traffic, and claimed that their workstations had been used by others without their knowledge - or that their PCs had been hijacked by malicious software. In some cases users openly admitted to downloading content for private gratification, but objected that there was no university policy to prohibit it.

In many cases, users had no idea of how much traffic they were generating. When informed, some of them were shocked and agreed to desist. Others shrugged their shoulders and questioned the right of the University to prohibit such activity. Some students insisted that since they were paying fees they had the right to download material for private purposes.

Policy, strategy, rules and regulations

It is important to recognise that policy, strategy, and rules and regulations are all different issues. They should, wherever possible, be dealt with separately. Although related and often closely linked, they are different in important ways. **Policy is not regulation,** and these two areas should be dealt with separately. Regulations are defined from the policy, and policy is derived from the strategy.

The relationships between these different components are important when developing effective policy. Consider the following four levels:

1. **Mission, vision, and values are about objectives.** What do we want to achieve? What are the visions or dreams of the organisation?
2. **Strategy is about the acquisition, development, deployment, and renewal of resources in the pursuit of objectives.** How are we going to get there?
3. **Policy concerns directed behaviour.** We define behaviour as either acceptable or unacceptable. By connecting these interpretations to our high-level definitions (or policy), we make decisions concerning where we want to go and how we plan to get there.
4. **Regulations are the codes of behaviour that policy will mandate.** So policy might say “the IT department shall from time to time set limits on traffic volumes” and the regulation might say “nobody may send an email

attachment larger than 3 Megabytes." Regulations are always made within the mandate established by policy, the do's and don'ts.

Each of these levels are distinct, but support the others. Access to network resources should support the mission of the organisation. Policy makers should develop an explicit strategy to make the best possible use of resources in support of that mission. The strategy is embodied in a published policy that defines acceptable behaviour on the part of network users. The policy is actually implemented through specific regulations that enforce proper behaviour, and define actions to be taken against users who violate the policy.

Real policy development at Havensburg

The University had always had an acceptable use policy for computer access, but it had been drafted in the 1990s and reflected the concerns of a pre-Internet IT department. The policy did not give the network administrators enough flexibility to monitor and manage the Internet connection to prevent abuse, so they convinced the University management to modernise it.

A task team was appointed to consult within the University and to consider the acceptable use policies of other institutions. The task team decided, as a point of departure, that the principle objective of policy was to ensure that Internet resources were used for institutional purposes: that is to say, it began with the assumption that not only the volume of traffic, but also the type of traffic, was relevant to its mandate. With this objective in mind, it embarked on a series of discussions with all academic boards and other institutional committees.

The task team pressed one argument repeatedly: that a minority of people were using the Internet for purely personal ends, and were also responsible for most of the traffic. They illustrated the argument with charts developed from analysis of the log files. They didn't promise that eliminating this traffic would also eliminate the congestion, but they did make a crucial point here: that if an Internet access circuit is being used solely for institutional purposes, and if it is congested, then it must mean that the University is not buying sufficient bandwidth. Every group to which the task team spoke agreed with this analysis.

The task team then drafted a policy, asserting that bandwidth was reserved exclusively for institutional purposes and expressly prohibiting its use for private purposes, and reiterating the University's commitment to respecting intellectual property rights in digital content. The draft policy was eventually approved by the University's board of governors and came into effect in 2002. A copy of the new policy was sent electronically to every student and staff member, and copies were posted in all public access computer facilities.

Characteristics of good policy

When developing a policy, it is worth considering the characteristics that differentiate good policy from bad. Below are details of such characteristics, they are generally policy independent and so are useful guidelines for the development of any policy.

- **Good policy has an enabling purpose.** The aims of the policy should be clear and apply to all users**.** If it is going to restrict user behaviour, then all users need to know why that is. This needs to be clearly stated and easily understood, as all users of your network need to understand this in order for the policy to be effective.

  The aims outlined in the the policy should not be a technical statement (e.g., "this policy exists to optimise the flow of data essential for our core business objectives over our network circuit."). Rather, it should be easy to understand and attempt to foster a collective responsibility towards creating positive network performance. For example:

  > "*Internet access is provided to achieve or sustain our business purpose. Using it for personal reasons compromises that goal by potentially slowing or halting important network services . This is why we have chosen to prohibit personal Internet use, except for the limited use described in [section y].*"

- **Good policy is linked to a wider objective.** Why is the policy trying to enable the above? The wider objective should relate to the bottom-line of the organisation. For example, a university might want to encourage education, teaching, and research. A human rights NGO's purpose might be about achieving their mission and objectives. These wider objectives should help focus people's attention on why network access is being provided. For example:

  > "*Internet service is being provided to allow human rights activists to consult appropriate online literature and not to download personal music collections.*"

- **Good policy has clear ownership.** Ownership of the policy should be clear and mandated from an appropriate level within the organisation. Ideally, this level will be that which is representative of all members of the organisation and not be seen as being imposed upon users by one part of the organisation. Wherever possible, the policy should be seen to be the will of the most senior management of the organisation, rather than the IT department, to increase its authority and effectiveness.

- **Good policy is short and clear.** If we want our users to abide by the policy, then they need to be able to read it. If we want them to buy into the policy (e.g., have all new students sign an agreement to abide by the ***Acceptable Use Policy*** (***AUP***)), then it must be easy for them to read and understand. The document should be clearly written and laid out. It should also avoid technical or legal jargon wherever possible.

- **Good policy arises from a valid process.** The process of how the policy was developed and put in place needs to be clear and easily understood by all members of the community it will affect. If it is seen as being imposed by the IT department without consultation, then will it be supported? The process should be clear and ideally show that opportunities for input and comment have been provided. A democratic process is more likely to achieve buy-in from all users.

- **Good policy works within the confines of a given authority.** Without the authority to make policy, it will be difficult to achieve buy-in from users and convince them to submit to the regulations. It is unlikely that a single network administrator can effectively set a policy for an entire university. But if the policy comes from the senate or university council, it is much more likely to be taken seriously. The authority should be above all users at whom the policy is aimed. In most cases, this should include all members of the community. In the case of a university, this includes faculty, staff, and administrators in addition to the student body.

- **Good policy is enforced.** The policy must be enforced and enforceable. If you do not consistently enforce it, then what happens when you do? Can a user claim unfair discrimination? Remember that enforcement is usually only an issue for a very small number of users who are disproportionately using your bandwidth. Evidence shows that enforcement can be achieved at both a technical level (e.g., blocking users or traffic) and a human level (sending a warning email). The simple human level warning is often effective.

- **Good policy is adaptable.** No policy is perfect; it may need revisions, particularly as the network grows. It is also important to provide clear information regarding how it can be changed or questioned. This need not be done in great detail, but it should be clear that the policy is not written in stone.

The new Havensburg network policy

The initial effect of the new policy was to reduce bandwidth consumption dramatically. Within a year, however, utilisation had begun to creep up again and response times were increasing. At this point the IT department was instructed to conduct another exhaustive analysis of log files. It identified six postgraduate students who were generating large volumes of traffic, the character of which was not apparent from the log files. The IT department lodged a formal complaint with the proctor, who instructed that the offending PCs be seized and their contents analysed. This demonstrated conclusively that the machines were being used to download pirated movies from a file sharing network. The students were charged with violation of university policy; two of them were eventually acquitted for insufficient evidence, and the other four were expelled. The findings of the disciplinary court were posted on the University's electronic notice board and prominently displayed in all public access computer facilities. The result was a sharp drop in circuit utilisation and a dramatic improvement in response times.

This respite was temporary, however: within eight months, utilisation was consistently above 95% during office hours, sometimes at 100%, and another investigation was undertaken. To the surprise of the investigators, there was no real evidence of abuse. A minority of users were still responsible for a majority of the traffic, but the material being transferred was large data sets that were integral to ongoing research. Coincidentally, a benchmarking exercise found that the University was purchasing only 60% of the bandwidth (adjusted for size) that equivalent peer institutions were purchasing. In light of this, The University Budget Committee agreed to release funds to increase the available capacity - but it also made it clear that it never would have made such an agreement unless it were also convinced that the University was no longer funding abuse.

Later that same year, researchers interviewing students and staff at Havensburg discovered that most members of the University community were satisfied with the speed of Internet access; most agreed with the University's acceptable user policy; most believed that they, as individuals, had a role to play in conserving bandwidth; most made a conscious effort to limit their own use of the Internet for private purposes. Most believed that any significant or sustained abuse would result in discovery, prosecution, and punishment. Very few were dissatisfied with this.

The moral of the story is that **Policy alone can't decongest a circuit**. But if applied vigorously, it can educate people, secure their support for limiting abuse, help to justify increases in expenditure that would otherwise never be supported, and sustain a culture of bandwidth conservation.

The policy development process

The policy development process is as important as the policy itself. The process is what will give the policy its validity and ensure that all members of the community understand why the policy is being developed, why the regulations exist, and will hopefully ensure user buy-in. Without an appropriate development process, a policy is likely to fail at some level.

The policy development process will be linked to the organisation's structure and culture. Some or all of the following issues should be considered.

- Understand your policy environment. Who has the authority to make policy? How can this authority be invoked?
- Understand your organisation's requirements for policy formulation and follow them. Are there specific consultation procedures that must be followed? Do specific committees or individuals need to give approval?
- Review the existing policy, if any exists. Consider conditions of service for staff policies on privacy. Any new policy should be in line with existing ones.
- Understand the wider legal environment. You cannot create policy that is in conflict with your legal system or your labour relations protocols. Some aspects of national law may have to be included in your policy (e.g., controls on access to pornography).
- Document the problem you're trying to solve and why policy is necessary to solve it. It can be useful to discuss the alternatives regarding improper use of the network and the limitations associated with it. This way, people see the need for the policy. **Why is policy necessary at all?** This is the most fundamental issue, and the message needs to be transmitted with absolute clarity.
- Document usage patterns. Typically, 5% of users account for 50% of the traffic. The other 95% of users should be on your side once they realise how they will benefit from the policy
- Document what has already been done to manage bandwidth problems. People are much more likely to be sympathetic if they believe that further policy and regulation are essential to improving their Internet access.
- Benchmark. If other institutions in the same class use policy as an instrument of bandwidth management, then mention this. It provides context and can be useful in competitive environments. (If other institutions are implementing specific policy then shouldn't we?)
- Identify who will support the policy and who might object. This will help you plan your response to objections as the policy is implemented. The documented usage patterns should be useful here.
- Identify the policy development team. It should include powerful figures who carry weight in the organisation. The chairs or deans of other departments might benefit the credibility of the developed policy, by being seen as independent of the Information Technology department.
- Communicate with your users. The policy development team needs to consult as extensively as possible with those who will be using the network. The consultation process is also a process for mobilising consensus concerning usage policies. Produce drafts of regulations and consult widely.
- Take time to navigate the policy approval process. Depending on the organisation, this may take a while.

- Plan for early wins. The process often raises plenty of expectations, so some tangible benefit should be delivered as soon as possible. This will show that progress is being made while broader changes are implemented.
- Make sure that the IT department is technically capable of doing whatever the policy will require.
- Enforcement is not the sole responsibility of the IT department. It must be supported by other processes, organizational structures, and ultimately the users themselves. Whatever the situation, the policy must be enforced, not because it is policy, but because the users recognise that it exists for the good of the network.
- Review the policy at set intervals. For example, create a schedule for policy review at three months after implementation and a year after implementation. Thereafter, repeat as necessary.
- Be proud of your results. Good results, when well advertised, are likely to help win over even the strongest opponents of the policy.

Policy is needed in all environments

Policies that guide bandwidth usage are not only the domain of low bandwidth environments. They are also an essential component of high speed networks. Experiences with very high speed networks show that, without policies and technical solutions, even multi-gigabyte (Gb) circuits can become congested and encounter degradations in performance. It was recently reported that up to half of the bandwidth at Finnish universities is used for downloading movies, music, and software. The network at Carnegie Mellon approached a gigabit of consumption before measures were taken to enforce an acceptable use policy.

In addition, there are very few contexts in which policy can be dispensed with entirely. People using a network affect other people's machines, whether they are in the same organisation or outside it. If users are handling corporate data of any kind, there are risks concerning loss, unauthorised modification, or unintended disclosure of sensitive or proprietary information. Therefore, some kind of policy is needed in order to manage those risks.

In general, you need policy to manage three specific kinds of risks: (**a**) risks arising from potential abuse, such as the excessive consumption of bandwidth; (**b**) risks arising from potential liability, arising out of things that users might do on networks (such as posting inflammatory or libelous remarks about other people); and (**c**) risks that arise out of a failure to comply with governmental regulations. These risks will vary considerably from one country to another, but there are very few contexts where they are completely absent.

Policy pitfalls

Your greatest danger lies in producing a vacuous policy - that is, a policy that is devoid of meaningful content. Policy must live in the heads of people, since its purpose is to shape or channel their behaviour. If it fails to do this, then it is a dead letter. Some examples of vacuous policy include:

- **Policy that is not backed by monitoring.** Ensure that you have the technical capability to monitor your network before you finalise policy. You should really have this ability at the start of the policy development process, since having a sense of the actual traffic is essential in order to build a realistic and relevant policy.
- **Policy that is unduly complex, or couched in legalistic language.** Policy is made for people, and needs to be kept focussed and readily understandable.
- **Policy that doesn't fit your environment, because it has been cut and pasted from somewhere else.** It's always best to write a policy from scratch and mobilise consent as you do so.
- **Policy that is not enforced, because of a lack of political will.** Unenforced policy is even worse than no policy at all, because it's much harder to reinvigorate a failed policy than it is to start a completely new policy process.
- **Unofficial policy.** Policy that does not have the backing of decision making structures of the institution, or that has been implemented in isolation, will be difficult to implement and will lack "teeth." When an unofficial policy arises that is in conflict with an approved "official" version, authority is undermined and users will choose to follow the rules that suit them.

Example policies

The following links provide good examples of issues covered by policy documents. Every organisation is unique and should develop policy that meets its own needs. The documents below can be useful when you reach the drafting stage of policy development, but you should never be tempted to skip the other stages – the process of creating workshops and consulting with community, concerning policy, is what educates them and secures their buy-in. You can often learn surprisingly important things from the user community regarding their needs. If you use someone else's documents during drafting, you should resist the temptation to cut and paste from them wholesale. Even the most generic policy needs some localisation. Editing existing policies invites inconsistency with your own network and how your community will use it. It's always best to write a policy rather than to copy one.

- The SANS institute policy template page:
  http://www.sans.org/resources/policies/#template
- A listing of policy examples from universities in the United States:
  http://ndsl.lib.state.nd.us/AcceptableUseExp.html
- The University of Cape Town's **Policy and rules on Internet and Email use** is a short policy that exhibits many key characteristics:
  http://www.icts.uct.ac.za/modules.php?name=News&file=print&sid=633
- Here is a longer policy that also includes most of the key characteristics: the University of KwaZulu-Natal's **ELECTRONIC COMMUNICATIONS POLICY**: *http://www.nu.ac.za/itd/policies/ecommunications.pdf*

Policy checklist

The two checklists that follow are provided to help with the development and implementation of effective policies to support bandwidth management and optimisation. Before you get started on this process though, make sure that you have documented the problem you're trying to solve (and why policy is necessary to solve it). You should also document usage patterns that support your case (see chapter three, **Monitoring & Analysis**).

Once you have done that, you should have a good sense of the nature of the problem from a social and technical point of view. You are now ready to start the policy development process (although, in reality, you will already have started it!). Remember, the policy development process is just as important as the policy it produces.

The policy development process checklist

✓ Understand your policy environment

✓ Understand your organisation's requirements for policy formulation and follow them

✓ Review existing policy

✓ Understand the wider legal environment

✓ Document what has already been done to manage the bandwidth problem

✓ Benchmark

✓ Identify who supports policy, and who doesn't

✓ Identify the policy development team

✓ Communicate with your users to understand their network experiences

- ✓ Produce a draft for consultation and consult widely
- ✓ Navigate the policy approval process
- ✓ Plan for early wins
- ✓ Ensure implementation and enforcement
- ✓ Gather feedback about network performance and policy requirements
- ✓ Periodically review the policy

Of course, a process is useless unless it produces an effective policy document and environment at the end. Be sure your policy exhibits all of the key characteristics found below.

Characteristics of good policy checklist

- ✓ Good policy has an enabling purpose
- ✓ Good policy is linked to a wider objective
- ✓ Good policy has clear ownership
- ✓ Good policy is short and clear
- ✓ Good policy arises from a valid process
- ✓ Good policy works within the confines of a given authority
- ✓ Good policy is enforced
- ✓ Good policy is adaptable

Once you have checked off all of the above, you will have a policy that provides an effective framework for bandwidth management and optimisation while having carefully considered the needs of your community.

References

- Illegal software and film downloads exhaust university computer networks, *http://www.hs.fi/english/article/1101978960379*
- Carnegie Mellon University case study, page **248**.
- INASP Bandwidth management and optimisation: policy development workshop, *http://www.inasp.info/training/bandwidth/bmo-pdw/*

Sample policy collections

- Educause collation on Acceptable/Responsible Use Policies: EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology, *http://www.educause.edu/content.asp?page_id=645&PARENT_ID=110&bhcp=1*

- Examples Internet Acceptable Use Policies: a large collection of example policies, mainly from US organisations. Including; Internet Acceptable Use Policies for Public Libraries; Internet Acceptable Use Policies for School Library Media Centers; Internet Acceptable Use Policies for Colleges and Universities, *http://ndsl.lib.state.nd.us/AcceptableUseExp.html*
- SANS Security Policy Resource page, a consensus research project of the SANS community. The ultimate goal of the project is to offer everything you need for rapid development and implementation of information security policies. You'll find a great set of resources posted here already including policy templates for twenty-four important security requirements, *http://www.sans.org/resources/policies/*
- Tech Republic: A framework for e-mail and Internet usage policies for your enterprise, *http://articles.techrepublic.com.com/5102-6299-1033914.html*