INASP: Effective Network Management Workshops

Unit 10: Policy Development

About these workshops

Authors:

- Dick Elleray, AfriConnect
    - delleray@africonnect.com
- Chris Wilson, Aptivate
    - chris + inaspbmo2013@aptivate.org

Date: 2013-04-29

Overview of Challenges and Solutions

Target participants

This workshop is specifically aimed at:

- ICT/Computer centre director * responsible for ICT policy development and implementation
- Other senior staff * responsible for the development and implementation of ICT policies
- Head librarians or senior library staff * involved in the development and implementation of ICT policies and should benefit from them

Introductions

Name, institution, role within your institution, questions:

- How many people in your IT department?
- How many computers on your network?
- How much bandwidth do you have?
- What is the biggest problem on your network?
- Any other areas that you would like us to cover?

If you are facilitating, you may wish to go round twice; once for the participants to introduce themselves, and then again for them to answer the questions above.

Content outline

- The role of a supportive policy environment
- Why policies often fail (examples of unsuccessful policy development)
- User authentication requirements and features
- Developing appropriate policies
- Sample policy review and development
- Planning an effective policy development process
- Writing an effective policy
- Implementing policy
- Policy implications and applications

Outcomes

- Examine the importance of a supportive policy environment for successful BMO
- Review key policies and an appropriate policy development framework
- Review BMO supportive policies
- Create an institutional level policy development action plan

Pre workshop task

- Request participants to bring five printed copies of their organisations “acceptable use policy” (AUP) relating to computers and the Internet * http://en.wikipedia.org/wiki/Acceptable_use_policy * These could include draft documents, working documents, implemented or planned policies, etc.
- Also include electronic copies if possible (e.g. MS Word, PDF, or website URL)
- **Please send electronic copies to the organisers in advance if possible.**

  http://en.wikipedia.org/wiki/Acceptable_use_policy

The State of Nature Game

Play the State of Nature Game described in the facilitators’ notes, to learn about public goods, free riding and collaboration vs. competition.

Rules of the game:

- The facilitator plays the role of Nature
- Each player begins the game with 100 Monetary Units (MU)
- In each round, each player must pay a survival cost of 10 MU
- Nature is bountiful and matches this amount
- The whole amount collected is auctioned off
- All bids are forfeit to the winner
- All agreements are permitted
- No agreements are binding
- No violence is permitted
- The object is to maximise your own outcome

Definition of a Public Good

A public good can be defined as:

- any good (resource or valuable thing)
- that the members of a community benefit from,
- irrespective of whether they have contributed to it, and
- which they can consume in arbitrary amounts (as much or as little as they wish to).

TCP/IP and Congestion

Understanding basic TCP/IP issues is important in understanding problems of overloaded and slow Internet connections:

- IP = Internet Protocol, basic protocol on which the Internet is built. * A “connectionless” and “unreliable” protocol.
- TCP = Transmission Control Protocol * A connection-oriented, reliable-transport protocol. * Adds (among other things) “flow control” to the IP layer. * When each TCP segments is received, an acknowledgement is sent back. * If a segment is not acknowledged then it is retransmitted by the sender.

TCP increases sending rate whenever no packets are lost. Thus it uses all the available bandwidth and causes congestion (deliberately).

Multiple connections share bandwidth “fairly” between them.

Congestion causes network collapse for all users; see Effect of Congestion in Unit 6 for details.

Policy and Behaviour

Technical measures alone fail to change behaviour. Why?

“5% of users use 50% of the traffic, so 95% should be on your side.” Discuss.

Policy and Behaviour

- Who has authority to create policy?
- Who has authority to implement technical measures?
- Who do users fear more?
- Whose side are the users on? What do they want?

Policy-based solutions

- Aim to bring about behavioral change
- Treat bandwidth just as any common good that needs policy management
- Can require or authorise use of technical solutions * distribute the bandwidth evenly between users * make sure that no one user can damage other users’ experiences * can prioritise and restrict traffic flows or users but which ones and how? * do not automatically ensure that the traffic that flows is consistent with institutional purposes

Examples of policy based approaches

Some simple examples, that we can come back to later.

A policy that says something about:

Appropriate and inappropriate use

Can be used to reward/punish such behaviour

Ability to limit traffic by volume

Can be used to set quotas

Ability to shape traffic

Can be used to throttle non-core online resources or speed up core ones

Virus protection and software standards

Can be used to remove problem computers/users from the network who do not comply

What makes a good policy?

Objectives

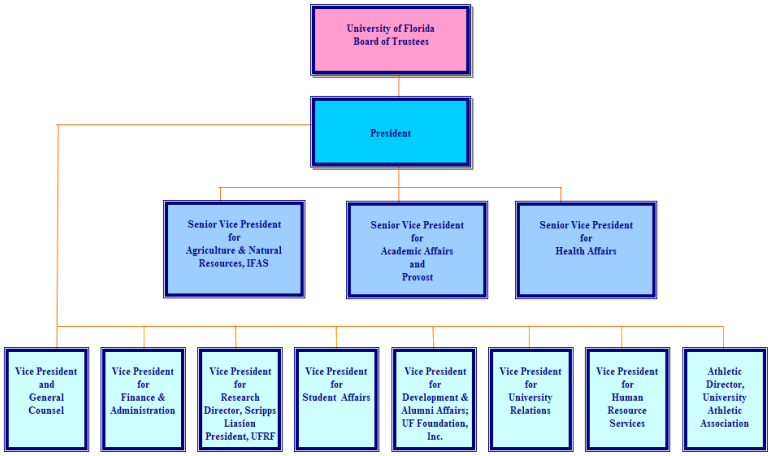
- Review the characteristics of good policy.
- Assess the degree to which the policy documents of participating institutions/other institutions meet the definition of good policy.
- Consider ways in which the policy documents can be improved.

What is policy, anyway?

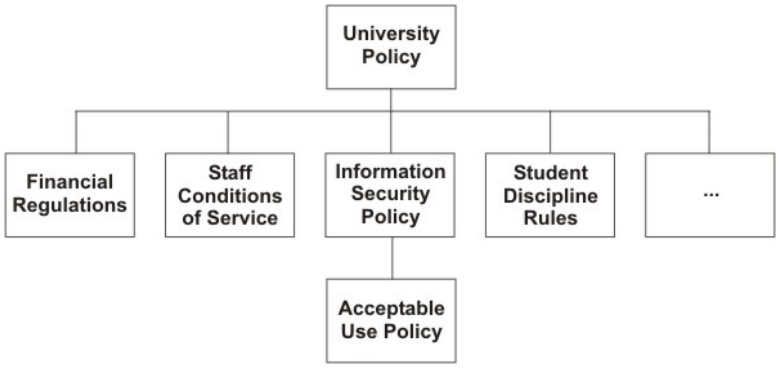
- Cognate terms: polis, police, political (with a small “p”)
- Who owns policy?

- How is it different from strategy?
- How is it different from regulations?

Example organisation structure



Note how the policy structure mirrors the organisation structure:



Authority is delegated down the tree, to write the rules governing some aspect of users' behaviour and interactions within the organisation.

Characteristics of good policy

- has an enabling purpose
- linked to a wider objective
- has clear ownership
- is clear and short
- managed by a process
- confined by a defined authority
- is enforced
- is adaptable

Good policy has an enabling purpose

- Policy is not just a set of restrictions.
- It is a set of restrictions with a purpose: * to make things possible
- It encourages and enables users, it is not just a list of do's and don'ts

Good policy is linked to a wider objective

- Why have the policy (at an institutional level)? * Why should I support this policy? * Be prepared for this question and be able to answer it
- The only way to win support for the policy * Rather than reluctant acceptance

Good policy has clear ownership

- Who owns the policy? * Is this clear from the policy document?
- Is it the “right” ownership to ensure support and buy in?
- It should not be the IT department * Imagine your plumbers making rules about what you can or can’t use your pipes for?
- It should generally be the highest authority in the institution that there is

Your plumber is providing a service to you, for a fee. They don’t own your pipes. You do, and you’re entitled to use them how you want. But you don’t flush poisons or machine oil down them, because that would be breaking the law.

Similarly, the IT department doesn’t own the Internet connection. It belongs to the unversity/organisation, and exists for the benefit of all, not just the IT department.

Good policy is clear and short

If we want it to be a live and useful document, then it should be:

- Clear and well written; no technical or legal jargon
- Short; easily read and digested by end users

You can have two versions if you really insist (one for all users to read and understand, and a supporting, full “legal” document) but not recommended! Just make one, short, simple, non-legal document.

Good policy arises from a process

- Processes are what secure buy-in and a sense of ownership
- Both essential for successful policy development and implementation
- Consensus is the process most likely to persuade all users * But the hardest to implement, for the same reason.
- Policy should not be static either! * Respond to changing needs of users. * The process needs to enable this, for example users propose amendments and they are voted on by a board.

Good policy is confined by a defined authority

Good policy works within the confines of a defined authority, for example:

> The IT department is authorised to restrict or suspend the access of some users, for limited time, to maintain the health of the IT services for other users.

Good policy is enforced

Good policy is adaptable

Finding the Policy

- What is the Acceptable Use Policy (AUP) for your network? Where is it?

- Ask someone who uses your network to outline the policy from memory. Compare it with the real policy.
- Ask someone to find a copy of it, and watch them try.

Consider how well your users understand your policy. Test them. Test the next person you see: is action X allowed by the policy or not?

How is your policy enforced, by who, and how well? Who follows the policy, who fights against it? How could you get them on side?

It's been said that "5% of users use 50% of the traffic, so 95% should be on your side." Do you agree? How many people abuse your network or cause problems for you? Do the others understand the problem and the benefits of reasonable, fair use? If not, how would you show them?

Who is responsible?

Who needs to be involved in network management, and why?

- Executive management
- Senior IT management
- Technical staff involved in the day-to-day implementation
- Academics, librarians and other legitimate Internet users

What roles do they play in managing a network?

Executive management

have the power to create or change policy and budgets.

Senior IT management

bridge the gap between staff on the ground, executives and the rest of the university.

Technical staff

have the skills to understand the problem, implement changes, and identify policy violations.

Legitimate Internet users

are the reason why the University pays so much for its Internet connection and the IT department. They are your customers!

Outline of a plan

- Simple overall aim * One to Three simple specific objectives * Simpler is safer (K I S S)
- An objective must be specific and measurable
- Justification * improving effectiveness * return on spend/investment
- Consequences * Of doing or not doing
- How do you manage risks during implementation * Go/No Go gates
- How will you monitor and review * Regular milestones
- Who are the key people (stakeholders)
- Timetable

Fair Deal

- Everyone gets 1 Mbps, without exception
- Pros: * Easy to implement * No policing required
- Cons: * Network resource will be under-used * Conversely, if everyone uses their 1 Mbps then capacity will be exceeded * Important work-related downloads may be slowed

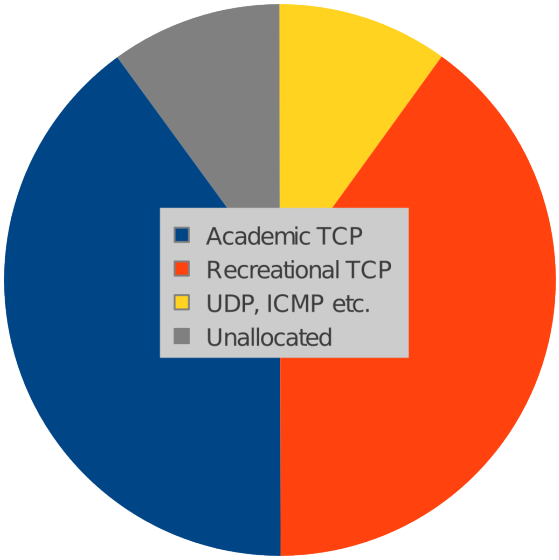
Punish repeat offenders

- Heavy users: * Those who transfer over 650MB/day off-campus are placed in heavy-user bucket * Heavy-users get limited bandwidth (e.g. 1.5Mbps aggregate) * Further reduction for repeat offenders
- Pros: * Heavy users get amplified negative feedback * No deep packet inspection required
- Cons: * Network resource will be under-used * Important work-related downloads may be slowed * Arbitrary limits are difficult to justify

Nuisance applications

- Define list of “nuisance” apps and identify their traffic
- All nuisance app traffic goes into a fixed bucket (e.g. 10 Mbps)
- Pros: * Low maintenance * Nuisance app users get amplified negative feedback
- Cons: * What is a nuisance app? How to identify it? * Users will discover new ways to abuse bandwidth * Requires a bandwidth manager with deep packet inspection

Protocol mix



- Academic TCP and Recreational TCP are “equal” * 40% each for Academic and Residential TCP
- Non-TCP and TCP don’t necessarily play well together * 10% for non-TCP
- Leave 10% unallocated (burst, control plane)
- Possible add-ons * Individual flow or user policing * Priority queuing
- Pros: * Low maintenance * Recreational users get amplified negative feedback
- Cons: * How to identify academic/recreational traffic? * Requires a bandwidth manager with deep packet inspection * Is 10% enough for VoIP applications and VPNs?