

Lanka Education and Research Network

Policy Framework

What? For Who? and How to?

12th June 2018

Workshop on Network Security - 2018

Thilina Pathirana

Based on and Credits: APNIC, APRICOT, NSRC, SANOG Security Tracks

LEARN

National Research and Education Network of Sri Lanka

Policy

How do your users know what is permissible?

How do you know what you can do?

Can you disconnect users from the network?

Can you eavesdrop on network traffic?

What do you include?

Typical policy framework for a University is an “Acceptable Use Policy” or AUP

Policy

Policy is an essential foundation of effective security program

The success of an information resources protection program depends on the policy generated, & on the attitude of management toward securing information on automated systems.

Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality.

Policies are important reference documents for internal audits & for resolution of legal disputes about management's due diligence

Policy documents can act as a clear statement of management's intent

Policy

Policies are least expensive means of control & often the most difficult to implement

Basic rules to follow when shaping policy:

- Never conflict with law
- Stand up in court
- Properly supported and administered
- Contribute to the success of the organization
- Involve end users of information systems

Policy

For policies to be effective, they must be:

- Properly disseminated
- Read
- Understood
- Agreed-to

Policy

Also the policies should clearly say who are the intended Audience

- Users
 - Students
 - Staff
 - General Public ?
- Administrators
 - Academics
 - IT Staff
 - etc...



Policy

- Keep policies short and clear – 1 or 2 pages
- Feel free to borrow from AUPs at other institutions
- Link to your existing disciplinary procedure
- Tell people where to go for help and advice
- All users must see, and preferably sign, the AUP
- Include this as part of an existing process (e.g. student enrolment or username/password setup)

Acceptable Usage

- Use of ICT resources for teaching, learning, research, administration or any other official activities of the University
- Personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others
- Advertising via electronic notice boards/forums, intended for this purpose, or via other University approved mechanisms
- However such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

Disallowed actions

- Causing annoyance, inconvenience or needless anxiety to others
- Unsolicited advertising, often referred to as "spamming"
- Sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address
- Attempts to break into or damage computer systems or data held thereon
- "You must not use anyone else's account, or allow your account to be used by anyone else"
- "You must keep your password secret. If you suspect someone else knows it, change it immediately"

Monitoring

- You should mention that users will be monitored. If you are doing the SSL inspection, then it should be clearly described.

“All use of the network and computing facilities is monitored and recorded for the purposes of enforcing this AUP. Your use of university facilities implies that you consent to your activity being monitored”

Consequences

“Failure to comply with this policy may result in your access to computing facilities being suspended or permanently withdrawn. It may also result in action being taken under the university disciplinary procedure, which could lead to expulsion”

Is it only AUPs???

Policies

- User Management Policy – user creation, modification, deletion
- Password Policy – Number of symbols, password expiry
- Wi-Fi Policy – where to access, who, how
- USB Policy – storage ?
- Computing Devices Purchasing Policy - Centralized Management
- Print / Photocopy Policy
- Single Sign On Policy – Develop Software to authenticate Using SSO
- Data Center / Network Room Access Policy
- Lab Access Policy

Group Activity / Discussion

Get in to groups of 6

Create a suitable AUP for your Institute

You may use, refer any internet material

Floor is also open for discussion

DEMO

Directory As A Service
(LDAP based user directory
supporting eduroam / edugain)

Lanka Education and Research Network

Thank You

Thilina Pathirana/LEARN

Email: thilina@learn.ac.lk