

A Reliable and Secure Network

**TM105: ESTABLISHING SANE
TECHNOLOGY POLICIES FOR
YOUR PROGRAM**

LSNY's Process

- Solicited Participation for All Offices and Job Classifications
- Reviewed User Policies from Other Legal Services Programs, Other Non-Profits, and Universities
- Shared the Draft Policy Program Wide for Comment
- Board Adopted the Policy

Considerations

- Workplace Free of Harassment
- More Secure Technical Environment
 - Protecting Client and Employee Data
- More Reliable/Consistent Technology Environment
- Supportive of Staff
- General Prohibition on Violating Applicable Laws
- Minimalist Approach

Internet Use

- May Use of the Internet for Personal Purposes
- Follows Our Practice of Non-Computer Resources
- General Prohibition Against Illegal Activity
- Reasonable Use - Don't Hog the Bandwidth
- May Not Install Software
- Lock Down the Environment
- Not Big Brother - Deal with usage problems as they affect the network, productivity, or other employees

Email

- Similar to the Telephone
- Big Security and Productivity Risks
- Getting Users to Think About Security
- General Prohibited Behavior
- Outside Email Issues
- Retention of Email

Steve's (in)Sane Approach

- **Open:** Don't put more energy into locking down your data than you do in securing your paper files. We really don't have anything that anyone wants anyway. Too much time, energy and expense can be put into security.

***Caveat:** this of course doesn't apply to ports outside your firewall or accessible to the internet. Hackers want your web or email server and they shouldn't be allowed to have it to torment others.*

- **Standards:** It is impossible to support every software application that a staff has an itch to try. pick a uniform set of core apps (email, browser, office suite) and install, support and train only those.
- **Freedom:** Program technology should not be controlled by the sys admins. The technology is present for the benefit of staff and their work. We should not lock down our systems to such a degree

Personal Use of Program Software and Hardware

To what extent can staff use the equipment for non work related activity?

LSSCM Policy:

Employees are permitted reasonable personal use of program equipment provided that: (a) this use occurs on that staff person's personal time; (b) the staff person reimburses the program for any direct costs associated with the use; (c) this use doesn't interfere or conflict with LSSCM's programmatic use of the property, equipment, or system.

User Responsibilities

In addition to prohibitions or limits on acceptable use, there are areas for which your program wants users to take affirmative responsibility.

- Storage & Back-up Considerations
- Regular Use of Email Mail and Voice Mail
- Virus Protection and Security
- User Control of Workstations

User Responsibilities (cont')

Data Storage

All staff should place case-related computer documents they work with in the appropriate common directories on the network share.

Regular Use of Email Mail and Voice Mail

Staff are responsible for checking and responding to voicemail and e-mail messages regularly. In general, communications through either of these systems should be checked at least daily. If you're not going to receive voicemail messages for longer than three days, you should leave a message to that effect on your voicemail. Voicemail and e-mail communications should be acknowledged and responded to as any other written communication or phone message.

User Responsibilities (cont')

Virus Protection and Security

Even with the best anti-virus software and security systems users can find ways to make a lot of work for others. Users need to be trained and then asked to take responsibility for their part in prevention.

- Email Attachments - some programs prohibit them and provide alternative means for file sharing. Some prohibit opening of a specific type (i.e. exe or pif).
- Passwords - most prohibit sharing of program passwords outside the program and some have standards for user selection and changing.
- Transporting Confidential Content on Electronic Media - most apply similar policies as paper case files.

User Responsibilities (cont')

Control over User Workstations

To what extent will you allow users to install software on their workstations whether for program or personal use?

LSSCM Policy:

All equipment is owned by LSSCM, therefore - Any material in any LSSCM system may be monitored, copied, or purged by the program management at any time.

Seek permission before installing software on your computer.

Currently LSSCM does not "lock-down" desktop computers to prevent software from being installed by individual users. However, users must get permission from both their managing attorney and the program wide CRP before installing additional software on their

Policy Resources

- Sane Technology Policies LSNTAP Training Module – Includes sample policies including LSNY and LSSCM.
- The [Entech NPO Tech Policy Template](#) is a free, online form based system that assists non-profits in creating their own program tech policy. Although it seems a *little on the restrictive side*.