November 18, 2008

Computer Resources Policies at the Center for functional MRI

1. Computer resources:
    a. Each PI is provided with an account with a 15G limit on one of the servers (cfmri or fmriserver).
    b. Each server has a guest account that can be used in case the other server is down. Data must be removed from the guest account when data transfer to an offsite server has been completed.
    c. Non-active accounts will be deleted one month after the PI's affiliation with the Center ends. The Center will notify the PI one week before deleting the account.

2. Data backup:
    a. Backup of the server accounts is mainly provided for disaster recovery; please do not depend on this for long term data storage and backup. Data should always be transferred from the Center's servers to the PI's computers as soon as possible. We also strongly recommend that PIs always back up their raw data on removable media using computers in their labs.
    b. Data on the scanner consoles (GE 3TW & 3TE and Bruker7T) is not backed up and can be deleted at any time by another scanner operator to free up disk space. Please remember to move the collected data (including Pfiles) to your server account. Verify that the transfer was successful by logging onto the server before you leave the scan room.
    c. Instructions for backing up of data to removable media are available on our website under the following URL:
        http://fmri.ucsd.edu/Howto/backupdata.shtml

3. Security (see also attachment 1):
    a. Remote access to our server is only available to UCSD addresses by request and closely affiliated academic institutions (such as SDSU and SALK) by request per IP address. Access from home has to be through a UCSD VPN connection.
    b. No one should be given access to CFMRI computers without first consulting with Eman Ghobrial, the Center System Administrator. All servers store critical data, and there is nothing worse than a physical breach.
    c. All servers have a virus scan and firewall software. PIs are responsible to make sure that their workstation is compliant with the minimum UCSD security requirements.
    d. We recommend that users reset their passwords to protect their data and our servers on an annual basis.

November 18, 2008

Attachment 1
Computer Security at the center

As of 1 January 2005, all devices attached to the UCSD network must meet the minimum standards for security, basically OS updates, virus scan protection and personnel firewall. For more information check the following site:
http://www-no.ucsd.edu/security/minstds/index.html

All Machines at the center now have some type of a firewall.

Windows
On windows we use the built-in firewall available for both Windows XP and Vista.

Macs
Macs have their own built-in firewall as well.

Linux/Unix servers and workstations
On Linux workstations we use IP Chains/tcpwrappers.
Traffic is allowed traffic for only SSH port (22) from UCSD and closely affiliated academic institutions (such as SDSU and SALK) by request only with IP address.
For remote access from home, use the VPN client. Information can be found at:
http://vpn.ucsd.edu

What is /Why firewalls?
A host-based firewall is software that runs directly on a networked device and protects that device against attack from the network by controlling incoming and/or outgoing network traffic. Host-based firewalls work by monitoring, passing, or blocking incoming and outgoing network packets. Rules govern what to look for and what to block or pass. Typical firewalls block based on source and destination address and port, packet type, etc.

Note that as of March 0f 2006 the ports (6000-6010) for X-forwarding should **NOT** be opened.

Please use the ssh command with the –Y options which tunnel the X-windows traffic over port 22 example:

ssh –Y <username>@<servername>
ssh –X <username>@<servername> (on older systems)

Passwords
Common passwords invite hackers and viruses to access your personal data. Increase your protection with these techniques:

- Use at least six characters although seven are preferable. Maximums and minimums vary with applications.
- Don't use names or words of more than four letters found in the dictionary. Try substituting numbers for vowels if your password is identified as a dictionary word.
- Avoid strings of numbers such as a birth date, social security number, or phone number.
- Mix upper- and lower-case letters.
- Include symbols in addition to letters and numbers.
- Avoid consecutive numbers or letters from the alphabet or keyboard.