UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF ECONOMICS
549 EVANS HALL # 3880
BERKELEY, CALIFORNIA 94720-3880

10 November 2003

STUDENTS, FACULTY, STAFF, AND VISITORS:

The Berkeley campus has adopted a new network security policy. We will make every effort to comply with the minimum standards of the new policy. A copy of our implementation guidelines and procedures is attached--as you read through them, you will find that most of them have been long-standing procedures in our department. What is new is the official campus security policy that outlines requirements for encryption of services like email, ftp, and telnet; centralized infrastructure scans to detect infected or "at risk" systems; and blocking of IP addresses to enforce compliance. I urge you to read the entire document.

In this context, "network devices" includes computers, printers, switches, and other equipment that connect to the campus computer network by cables or wireless. You are the system administrator of your own machine unless formal alternative arrangements have been made. You are responsible for the security of your system and for any attacks that may be launched from your system.

- If you manage your own computer, you should do Windows security updates to your operating system and applications on a regular basis. We recommend that you set your system to do this automatically once per week. For Windows XP, right-click `My Computer-> Properties-> Automatic Updates`. Click on `Automatically download the updates and install them on the schedule that I specify` to enable this feature, and select a day and time *when you are sure that your computer is turned on and connected to the internet* from the drop down menus that are provided. Configuring other Windows operating systems may vary slightly, but the principle is the same.

- The new campus policy requires that antivirus software must be installed on all computers, and checks made for updates on a regular basis. If you manage your own computer, we recommend that you do this at least once per week for desktops and daily for laptops, and that you *configure the software for active checking of new and accessed files on demand.* For people who use the campus license of Symantec's AntiVirus CE software for Windows XP, turn on `Enable File System Realtime Protection`. To do this, open `Start -> Programs-> Symantec Client Security-> Symantec AntiVirus Client`. In the control panel, open `File-> Schedule Updates` and click on `Enable scheduled automatic updates`. In the dialog box provided, click on `Schedule` and select a schedule for your Symantec Live Updates. Again, be sure to select a day and time when you are sure that your computer is turned on and connected to the internet. Configuring SAVCE for other Windows operating systems may vary slightly, but the principle is the same.

- Passwords must be kept secret and must be sufficiently complex to be secure. We have always encouraged this practice in the past; however, the campus is now developing a new policy that will define password complexity standards to which we all must comply. There is no exception to the "secret and complex" rule.

- If you run a local FTP, HTTP, TELNET, RSH, REXEC, or SMTP service on your own, *read the attached procedures carefully*. The campus now requires that *server* services must be provided securely, meaning that you must use accepted security standards like SSL, SSH, and SFTP that encrypt all activity. In addition, if you provide *server* services, your users must be properly authorized to use your service, as well as properly authenticated, using standard user account management practices.

- If you manage your own computer, we recommend that you switch now to SSL-enabled mail clients. Eudora, Netscape, Mozilla, and Pine are all compatible, so you should configure them to enable SSL. Within one year from this date, the Econometrics Laboratory will cease support of unsecured `pop` and `imap` service from both outside *and inside* the Berkeley.EDU domain. This is a central campus requirement for all mail service providers.

- Do not leave your machine logged on and unattended for extended periods. Lock the console and ensure that your door is locked when your office is not occupied. For those of you who manage your own computers with Windows operating systems, "lock the console" means, for example, (a) enable password protection for your computer, (b) logout if you leave your office, (c) do `Control-Alt-Delete` and click on `Lock Computer` as an alternative to a logout, or (d) configure a screen blanker for a 30-minute idle time with password enabled. For item (d), you can right-click on a blank area of your desktop, and select `Properties`. Click on the `Screen Saver` tab and choose a screen blanker from the drop down menu. Set `Wait` to `30` and click on `On resume, password protect`. For staff and student computers that are idle, we will comply with the new campus policy by implementing password-protected screen blankers and forced logouts on all systems managed by the departmental IT staff.

- With the exception of managed student and staff systems, you and your invited guests and visitors must supply your own media and licenses. The Econometrics Laboratory and the Economics Department will not supply installation media for applications and operating systems because of license and copyright restrictions.

- Regardless of whether you manage your own computer or if it is a departmental system, you may *not* assign your network address to another computer, resurrect a disconnected computer, or connect a new computer, without consulting our IT staff first. Make an appointment *at least one week in advance* with the IT staff to accommodate your needs or the needs of your visitors.

- In compliance with the new security policy, unannounced physical and electronic checks on equipment attached to the network will be made by central campus security administrators and the department's IT staff. Non-compliant or compromised systems will be immediately disconnected or will have their IP address blocked or both. Owners of "at risk" systems will be notified and given an opportunity to update and patch their computers. "At risk" computers will be disconnected if they are not updated in a timely manner.

I believe that these guidelines come as no surprise to anyone, because the campus has been moving toward a more secure computing environment over the past few years. I encourage everyone to read the attached departmental policy carefully, and ask that you make a good faith effort to comply with Berkeley campus security guidelines.

Richard Gilbert
Chair