UNIVERSITY OF CALIFORNIA, BERKELEY

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

SANTA BARBARA • SANTA CRUZ

ECONOMETRICS LABORATORY
Institute of Business and Economic Research

ECONOMETRICS LABORATORY &
DEPARTMENT OF ECONOMICS

IMPLEMENTATION POLICY AND PROCEDURES FOR SECURING NETWORKED DEVICES

01 November 2003

Statement of Scope

This departmental policy applies to networked devices on the Econometrics Laboratory and Department of Economics network infrastructure including, but not limited to, subnets 128.32.105 and 169.229.128 and the Laboratory's dialup modem service. It extends, but does not supercede, applicable Berkeley campus policies.

Applicable Berkeley Campus Policies

- Berkeley Campus Information Technology Security Policy [http://socrates.berkeley.edu:2002/IT.sec.policy.html]
- Minimum Standards for Security of Berkeley Campus Networked Devices [http://socrates.berkeley.edu:2002/MinStds/]
- Specific Platform Password Complexity Guidelines [in progress]
- Berkeley Campus IT Security Policies and Guidelines [http://socrates.berkeley.edu:2002/pols.html]
- Guidelines for Administering Appropriate Use of Campus Computing and Network Services [http://itpolicy.berkeley.edu/approp.use.html]

Daniel McFadden, Director
655 Evans Hall
Tel: (510) 643-8428
Fax: (510) 642-0638
mcfadden@econ.Berkeley.EDU

Mailing Address:

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

Grace Katagiri, Manager
643 Evans Hall
Tel: (510) 642-8724
Fax: (510) 642-0638
katagiri@econ.Berkeley.EDU

Implementation Guidelines

These guidelines are based upon "Minimum Standards for Security of Berkeley Campus Networked Devices" [http://socrates.berkeley.edu:2002/MinStds/] .

1. Software Patch Updates

All networked devices are expected to have all hardware and software security patches installed that address any security vulnerabilities. Exceptions may be made for patches that compromise the usability of *system-critical* applications after review and approval by the departmental IT staff.

2. AntiVirus Software

Currently available and reliable antivirus software is expected to be installed and kept updated on every level of device, including clients, file servers, mail servers, and other types of networked devices. The minimum standard for antivirus software is to meet or exceed the effectiveness standards of those site-licensed by UC systemwide or the Berkeley campus. [See http://software.berkeley.edu .]

3. Passwords

Campus electronic communications service providers are required to have a suitable process for authorizing any use of shared electronic communications services under their control. The Econometrics Laboratory and the Department of Economics provide access through use of password-protected user "accounts" and other secure authentication system standards. These standards include, but are not limited to, secure shell in place of open telnet; secure FTP and browser-enabled FTP in place of open FTP; limited anonymous FTP; secure copy in place of remote copy; CalNet (Kerberos) authentication; SSL encryption for web and email.

Where allowable by the operating system, passwords are enforced that meet complexity ("strong") requirements specified in "Specific Platform Password Complexity Guidelines".

All default passwords for network devices and for network-aware software residing on network devices in the Econometrics Laboratory and Department of Economics are required to be modified immediately without exception when first configured and installed. Some network-aware software and some network devices may be pre-installed by the vendor with default passwords. No devices may be connected to the network with default passwords, and no network-aware software may be installed on network devices with default passwords. Non-compliant devices will be disconnected and will not be permitted back on the network until the default password has been replaced with a strong password by the owner.

The Econometrics Laboratory and the Department of Economics are service providers and device administrators under the definitions of the Minimum Standards for Security of Berkeley Campus Networked Devices. We are therefore required to, and are in compliance with, provisions that require creation of local password or other secure authentication system standards, including requiring that all shared system users meet

Daniel McFadden, Director
655 Evans Hall
Tel: (510) 643-8428
Fax: (510) 642-0638
mcfadden@econ.Berkeley.EDU

Mailing Address:

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

Grace Katagiri, Manager
643 Evans Hall
Tel: (510) 642-8724
Fax: (510) 642-0638
katagiri@econ.Berkeley.EDU

these standards. Users are responsible for the security and appropriate use of their accounts. Accounts will be revoked and all system and network privileges denied to any user who shares account login and password information with anyone.

Passwords for privileged access by systems administrators and local administrators are not permitted to be the same as those used for non-privileged access.

4. No Unauthorized, Unencrypted Authentication
Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network is subject to authorized and unauthorized monitoring, rendering these authentication mechanisms vulnerable to compromise. The campus therefore requires that all devices must use only encrypted authentication mechanisms. The Econometrics Laboratory and the Department of Economics have, for many years, disabled insecure telnet, FTP, and remote copy. The Econometrics Laboratory's SMTP server has also denied POP downloads to any systems outside the Berkeley.EDU domain, and has required IMAP with SSL enabled for mail clients on systems outside the Berkeley.EDU domain. ***Within one year from this date, we will require all POP and IMAP access to be secure.*** Unsecured POP and IMAP, even from inside the Berkeley.EDU domain, will be prohibited.

5. No Unauthorized, Open Email Relays
The Department of Economics provides no mail service. The mail service of the Econometrics Laboratory has, for many years, denied unauthorized third party message relaying, that is, the SMTP server will not process any email messages where neither the sender nor the recipient is a local user. We will continue this practice.

6. No Unauthorized, Unauthenticated Web Proxies
The Econometrics Laboratory and the Department of Economics maintain no web proxy services. If we should implement such a service in the future, it will be in full compliance with current campus standards.

7. Physical Security
Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or compromises involving privacy issues with potential legal consequences. We strongly recommend that all users logout of systems that will be unattended for thirty minutes or longer, and that doors are securely locked when offices are unoccupied.

For managed devices in field research offices and in the open "Park Avenue" laboratory, the Economics Department will enforce a combination of screensaver locking, forced logouts, and system reboots when devices are idle. For managed devices in staff offices, the Economics Department will force screensaver locking when devices are idle, and will force logouts and system reboots once a week. System reboots will be timed for minimal disruption of normal working activities, but will be enforced without exception for managed devices.

Daniel McFadden, Director
655 Evans Hall
Tel: (510) 643-8428
Fax: (510) 642-0638
mcfadden@econ.Berkeley.EDU

Mailing Address:

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

Grace Katagiri, Manager
643 Evans Hall
Tel: (510) 642-8724
Fax: (510) 642-0638
katagiri@econ.Berkeley.EDU

8. Unnecessary Services
If a service is not necessary for the intended operation of the device, that service should not be running. All Econometrics Laboratory and Department of Economics managed devices will be configured accordingly. Networked devices that are not managed by departmental or laboratory systems administrators are said to be *unmanaged*. The owners of unmanaged devices are the system administrators responsible for their devices.

Implementation Procedures

Networked devices that are not under the direct management of the IT staff are self-administered by their owners. The policies and procedures outlined in this document apply to departmental systems administrators and to owners of unmanaged systems who are their own system administrators.

No network device may be connected to the Econometrics Laboratory and Department of Economics network infrastructure until it is in full compliance with the following criteria:

- ***The network device must meet or exceed the minimum security requirements*** defined by the Berkeley campus Systems and Network Security (SNS) office [http://security.berkeley.edu] and by the Berkeley campus Communications and Network Services (CNS) policies and guidelines [http://cns.berkeley.edu].

- ***The network device must be checked and properly updated and patched for known vulnerabilities prior to enabling connectivity.*** New systems "right out of the box" are automatically vulnerable.

- ***The network device must have strong passwords enabled that meet or exceed "Specific Platform Password Complexity Guidelines" requirements***. Where permitted by the operating system, use nine or more characters, and use three or more character sets (upper case, lower case, punctuation, numerals, control or extended characters).

- ***Current antivirus software must be installed on all network devices that meet or exceed the effectiveness of antivirus software that is site licensed by UC systemwide or the Berkeley campus*** [http://software.berkeley.edu]. The software must be configured to update no less than once a week for always-on desktops, and daily for laptops or periodic-use desktops.

- ***Software updates for network devices must be checked at least once a week. Critical updates must be applied immediately.*** Auto-updating is advisable. Laptops, which are often disconnected, should check daily with at least a 12-hour retry period.

Daniel McFadden, Director
655 Evans Hall
Tel: (510) 643-8428
Fax: (510) 642-0638
mcfadden@econ.Berkeley.EDU

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

Grace Katagiri, Manager
643 Evans Hall
Tel: (510) 642-8724
Fax: (510) 642-0638
katagiri@econ.Berkeley.EDU

- ***Network devices may not run unnecessary services***, unless they are designated production servers managed by departmental systems administrators. ***Exception:*** Unmanaged systems administrators may run *server* services under the following conditions: (1) Notify the IT staff of all *server* services that are running on their networked devices. These may include, but are not limited to, FTP, SSHD, POP, IMAP, SMTP, HTTP(S), and peer-to-peer file sharing. (2) Complete and sign a "Statement of Personal Management Responsibility for a Networked Device" with the IT staff. During routine security checks, unmanaged systems running server services that have not been registered will be disconnected without warning.

- ***Visitors must own their own software licenses and installation media***. The Econometrics Laboratory and the Department of Economics will not provide installation media for operating systems and applications software, because of copy protection and licensing restrictions. Visitors are expected to bring their own master media and license keys with them if they travel with their own network devices.

- ***Network address assignments must be reviewed and approved by the IT staff prior to system configuration***. Incorrect or duplicate addresses cause network problems. Substituting a system on a network connection may affect the security status of the registered user of that connection, which may include the blocking of the network address and the removal of all account privileges. Therefore, no new devices may be connected to departmental infrastructure without first being validated by the IT staff. Any device that has been disconnected for longer than one month may not be reconnected without first being validated by the IT staff. Appointments for hardware testing and validation of operating system and applications software must be made one week in advance with the IT staff (*nthelp@econ.berkeley.edu; 643-5397*).

- ***The Econometrics Laboratory and the Department of Economics reserve the right to periodically and without prior notification engage in physical and electronic security checks of all networked devices*** including, but not limited to, wired hosts on subnets 128.32.105 and 169.229.128, and remote hosts utilizing the Laboratory's dialup modem service. Networked devices that are noncompliant or pose a security risk will be disconnected. Unmanaged devices that are blocked by SNS are the sole responsibility of the owner, and will require the owner to interact personally with the SNS office to restore connectivity.

The Econometrics Laboratory and the Department of Economics will revoke all user account privileges for individuals whose networked devices are found to be in noncompliance, are being used for malicious purposes, or whose security is otherwise compromised.

Daniel McFadden, Director
655 Evans Hall
Tel: (510) 643-8428
Fax: (510) 642-0638
mcfadden@econ.Berkeley.EDU

Mailing Address:

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

Grace Katagiri, Manager
643 Evans Hall
Tel: (510) 642-8724
Fax: (510) 642-0638
katagiri@econ.Berkeley.EDU