UCLA Policy 401 Minimum Security Standards for Network Devices

Issuing Officer:	Administrative Vice Chancellor
Responsible Dept:	Administrative Vice Chancellor's Office
Effective Date:	June 3, 2010
Supersedes:	UCLA Policy 401, dated 11/22/2005

I. INTRODUCTION AND PURPOSE

UCLA encourages the use of its electronic communications network in support of the University's mission. However, this resource is limited and may be vulnerable to attack or improper use. It must be well-managed and protected, and UCLA reserves the right to deny access to its electronic communications network by Devices that do not meet its standards for security.

The purpose of this policy is to establish the Minimum Security Standards for all electronic Devices connecting to the UCLA Campus Network, in accordance with the principles endorsed by the UCLA Information Technology Planning Board March 31, 2005. Such standards serve to help protect not only the individual Device, but other Devices connected to the Campus Network. Portions of this policy are drawn from the UC Berkeley Minimum Security Standards for Networked Devices, issued January, 2004. This policy also identifies those with principal responsibility for compliance with the Minimum Security Standards, and for the enforcement of this policy, including taking corrective action.

II. DEFINITIONS

For the purposes of this Policy:

Campus Network: All UCLA networks connected to the campus backbone network, directly or indirectly, and whether or not behind a firewall or Network Address Translation (NAT) device. (NAT is an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic).

Connectivity Service Provider: A unit, organization, or person that enables access to the Campus Network by UCLA faculty, students and staff and including for visiting scholars, conference attendees or other temporary visitors to UCLA.

Network Device (Device): A computer, printer, wireless appliance or other piece of equipment that can connect to and communicate over the Campus Network.

System Administrator: An individual who installs, configures and/or maintains any Device in his or her area of responsibility that is connected to the Campus Network.

III. STATEMENT

This policy applies to all faculty, staff, students and contractors who connect a Network Device to the Campus Network. (i.e., when a Network Device will be assigned an Internet Protocol (IP) address that is routable on the Campus Network and, can be used to send data to, or receive data from, the Campus Network). This policy is applicable:

- regardless of how the Device is connected to the Campus Network (e.g., directly from a campus office or indirectly from a faculty member's home, for example using the UCLA wireless or the UCLA Virtual Private Network (VPN)); and
- whether or not the Device is owned by the University.

Whenever anyone is connected to the Campus Network, he or she is expected to comply with this Policy.

A. Compliance with Minimum Security Standards

All Devices connecting to the Campus Network, whether physically located on campus property or not, must comply with the Minimum Security Standards in Attachment A. A Device that does not meet these Minimum Security Standards is subject to disconnection or having its access blocked to the Campus Network until remediation has been performed. More restrictive standards may be adopted at the department or unit level.

Devices that host restricted data as defined in University of California Business and Finance Bulletin IS-3 may be required to conform to more rigorous security standards. Devices hosting specific types of data (e.g., as defined by UCLA Policy 420, the Health Insurance Portability and Accountability Act (HIPAA) or the Payment Card Industry Data Security Standard (PCI-DSS)) may be subject to additional constraints. See the "Protection of Personal Information" Web site https://www.it.ucla.edu/security/protecting-personal-information-resources for guidance.

B. Responsibilities for Compliance and Enforcement

System Administrators

System Administrators shall ensure that every Device for which they are responsible is in compliance with the Minimum Security Standards.

A System Administrator may be an IT staff member whose responsibilities include ongoing maintenance for all Devices in a department or computer lab. A faculty member functions as a System Administrator when his or her personally owned computer at home connects to the Campus Network (e.g., via the UCLA wireless or through the UCLA Virtual Private Network (VPN)).

Connectivity Service Providers (CSP)

Connectivity Service Providers shall take appropriate corrective action:

1. when a Device connected to the Campus Network is causing disruption (e.g., sourcing a denial-of-service attack). In such situations, the CSP must have procedures in place to identify the problem Device and disconnect or block its access as appropriate. The Device may be reconnected only when the cause of the disruptive behavior has been addressed *and* provided it meets the Minimum Security Standards. Further, if the Device hosts personal information as defined in UCLA Policy 420, a potential security breach must be assumed and the procedures in that policy must be followed.

2. if a Device connected to the Campus Network is found not to meet the Minimum Security Standards (e.g., through a vulnerability scan). In such situations, the Device is subject to disconnection or having its access to the Campus Network blocked by the CSP unless remediation is completed in a timely manner.

Under certain circumstances, a CSP may execute approved alternatives to the Minimum Security Standards, as listed in section C., below.

C. Exceptions to the Minimum Security Standards

A Device may connect to the Campus Network only if it meets the Minimum Security Standards. However, there may be various reasons why a Device does not meet these standards yet has a legitimate reason why it needs to connect to the Campus Network. In such cases, under the following circumstances, an exception may be made by employing alternate security measures.

1. Many common Devices either do not meet these standards (e.g., printers with a built-in web server) or it would be impractical for critical usability reasons (e.g., grid computers, some high-volume servers). In such cases, standard alternate security measures can be employed, thereby satisfying the Minimum Security Standards (See Attachment B).
2. Laptops and other Devices brought by visiting scholars, conference attendees and other temporary visitors to UCLA cannot be assumed to comply with these Minimum Security Standards. Therefore, a CSP must develop an appropriately secured environment in order to provide access to the Campus Network for such visitors.
3. Any other Device that cannot meet the Minimum Security Standards may still be connected to the Campus Network if an alternate method of providing equal or greater security is documented by the System Administrator and this alternate method is approved by the Connectivity Service Provider.

All exceptions shall be documented in writing (electronically or otherwise) and kept on file by the Connectivity Service Provider. Such documentation shall be kept on file for as long as the Device associated with the exception is connected to the Campus Network.

D. Recourse

Appeals concerning decisions made or actions taken by a Connectivity Service Provider may be made to the Administrative Vice Chancellor, who will consult with other campus officials, as appropriate, to make the final determination.

IV. REFERENCES

1. UC Business & Finance Bulletin IS-3, Electronic Information Security;
2. UCLA Policy 420, Notification of Breaches of Computerized Personal Information;
3. UCLA Procedure 350.6, Campus Backbone Network (CBN);
4. Health Insurance Portability and Accountability Act;
5. Payment Card Industry Data Security Standard.

V. ATTACHMENTS

A. Minimum Security Standards for Network Devices.

B. Implementing Guidelines for Minimum Security Standards for Network Devices.

Issuing Officer

/s/ Sam J. Morabito

Administrative Vice Chancellor

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.

Minimum Security Standards for Network Devices

These minimum standards are intended to ensure the security of all Devices connected to the Campus Network. Any Device to be connected to the Campus Network must satisfy the following minimum standards, as appropriate, or adopt a standard alternate security measure (see Attachment B).

1. Software patch updates

Devices to be connected to the Campus Network must run software for which critical security patches are made available in a timely fashion and must have all currently available security patches installed.

Exceptions may be made for patches that compromise the usability of critical applications.

2. Anti-malware software

Anti-malware software for any particular type of operating system must be running and up-to-date on every Device, including clients, file servers and mail servers. Products other than offered by the campus may be used if comparable.

Exceptions may be made for anti-malware software that could compromise the usability of critical applications.

3. Host-based firewall software

System Administrators are responsible for ensuring that computers with native host-based firewall software included in the operating system have the firewall activated and properly configured.

Exceptions may be made for firewall software that compromises the usability of critical applications.

4. Passwords

Campus electronic communications systems or services that require users to be identified must identify and authorize users using secure authentication processes (e.g., digital certificates, biometrics, Smart Cards, one-time passwords or encrypted password transactions). When reusable passwords are employed, they must meet the minimum password complexity standards below. In addition, shared-access systems must be configured to enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible Devices must be modified.

Passwords that may be used by System Administrators for their personal access to a service or Device must not be the same as those used for privileged access to any service or Device.

All passwords employed to authorize access to campus electronic communications systems or services must meet the following minimum password complexity standards. The password *must:*

- Contain eight characters or more.
- Contain characters from at least two of the following three character classes:
    - Letters (a-z, A-Z)
    - Numbers (0-9)
    - Special characters including a space (: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

5. Unencrypted authentication

Unencrypted Device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the Campus Network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. To prevent password harvesting, passwords must not be sent in the clear and all campus Devices must use encrypted authentication mechanisms or otherwise secure authentication mechanisms. Passwords or protocols which provide no log on access to the system (e.g., anonymous FTP) are exempted from this requirement.

6. Unauthenticated email relays

Campus Devices must not provide an active SMTP (an Internet protocol for sending email between Devices) service that allows unauthorized parties to relay email messages. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Unless an unauthenticated relay service has been reviewed by Information Technology Services as to configuration and appropriate use, it may not operate on the Campus Network.

7. Unauthenticated proxy services

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate Device configuration.

Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by Information Technology Services as to configuration and appropriate use, it is not allowed on the Campus Network.

In particular, software program default settings in which proxy servers are automatically enabled must be identified by the System Administrator and re-configured to prevent unauthenticated proxy services.

8. Physical security

Unauthorized physical access to an unattended Device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, Devices must be configured to “lock” and require a user to re-authenticate if left unattended for more than 20 minutes.

System Administrators are responsible for maintaining the physical security of devices in their care.

9. Unnecessary services

If a service is not necessary for the intended purpose or operation of the Device, that service shall not be running.

Implementing Guidelines for Minimum Security Standards for Network Devices

These Guidelines are intended to assist System Administrators and Connectivity Service Providers in achieving compliance with the Minimum Security Standards for Network Devices. Departments may choose to adopt higher standards of security for Devices than those stated in Attachment A if they are compliant with the UC Electronic Communications Policy and other relevant campus and University policies.

A. Non-compliance with Minimum Security Standards

An alternative to disconnecting a Device or blocking its access to the Campus Network is to put it into a quarantine area, providing users with limited access or a web-based service to assist with checking, updating or cleaning the Device.

Connectivity Service Providers should make System Administrators aware of the Minimum Security Standards.

When investigating a security incident, Connectivity Service Providers should also check the security of any other Device to which the compromised machine was connected.

B. Exceptions to the Minimum Security Standards

Many common Devices do not meet the Minimum Security Standards (e.g., printers with a built-in web server) or for some Devices it is not appropriate or practical to meet them for critical usability reasons (e.g., grid computers, some high-volume servers). In such cases, standard alternate security measures can be employed instead, thereby satisfying the fundamental requirements of the Minimum Security Standards. Use of these alternate methods should generally be automatically approved by a Connectivity Service Provider.

Device or System Standard Exception	Security Actions for Automatic Approval by CSP
Network printers	Redirect HTTP traffic
Servers with critical applications that would be impacted by one or more of the Minimum Security Standards	Firewall, change management, enhanced system monitoring
Older operating systems that cannot be upgraded	Firewall, change management
Devices that cannot fully implement the minimum password complexity standards	Use the strongest password possible within the restrictions of that particular system.

C. Software patch updates

Patch management software is available for Windows computers at discounted rates by going to the UCLA Software Central site at www.softwarecentral.ucla.edu. Alternate patch management software may be used if comparable.

D. Anti-malware software

Anti-malware software is available free of charge to all UCLA faculty, students and staff (including personally owned computers) by going to www.bol.ucla.edu/software/sophos. Anti-malware software is required for an operating system if it is listed as "Supported" on the web page noted above. If an operating system is listed as "Unsupported," then it is only recommended that such software be used. Alternate anti-malware software may be used if comparable.

E. Passwords

Campus electronic communications systems or services that require users to be identified must identify and authorize users using secure authentication processes. However, this does not preclude anonymous access to such services where appropriate. Anonymous access does not exempt a Connectivity Service Provider from the requirement to have procedures in place to identify and isolate problem Devices on a network.

In cases where a Device cannot implement the minimum password complexity standards (see Passwords in Attachment A), the strongest requirements that can be used within the restrictions of that particular system shall be used.

Some user guidelines for avoiding poor passwords:

- Names of family, pets, friends, or co-workers.
- Names of well-known fictional characters.
- Computer terms and names, commands, sites, companies, hardware, or software.
- Birthdays or other personal information such as addresses or phone numbers.
- A set of characters in alphabetic or numeric order (e.g., abcdef), in a row on a keyboard (e.g. qwerty), or in a simple pattern (e.g., 123123).
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., qwerty1, 1qwerty).
- A bank account PIN.

F. Unencrypted authentication

There are some situations where encrypted passwords are inappropriate or irrelevant. For example, for use with anonymous FTP or one-time passwords.

G. Unauthenticated proxy services

Unauthenticated proxies have implications for content licensed by UCLA for the UCLA community. Therefore, if Information Technology Services approves an unauthenticated proxy service, it shall notify the UCLA Library that it has done so in order that the Library may block access from the appropriate addresses. Other units with such licensed content should contact Information Technology Services to be notified as well.

Proxy servers must conform to this policy. Devices that connect to the UCLA Campus Network only through a proxy server are not subject to this policy.

H. Unnecessary services

Systems Administrators should actively configure a system, making judgments about the services that must be available on the Device so that it meets its intended purpose or use, and eliminating unnecessary services.