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.