University of California, Merced

Minimum Security Standards for Networked Devices

Responsible Official:	Chief Information Officer
Responsible Office:	Information Technology
Issuance Date:	
Effective Date:	
Summary:	Minimum requirements for connecting devices to the UC Merced research and housing networks.
Scope:	Faculty, Staff, Students, Affiliates

Contact:	Ann Kovalchick, Chief Information Officer
Email:	akovalchick@ucmerced.edu
Phone:	(209) 228-4899

I. REFERENCES AND RESOURCES

UC Policies

- IS-3 Electronic Information Security
- Electronic Communications Policy
- UC Merced Acceptable Use Policy

II. POLICY/PROCEDURE SUMMARY & SCOPE

The University is committed to protecting information and complying with regulations and policy related to security and acceptable use of electronic information. Access to and use of campus network services are privileges accorded at the discretion of the University of California, Merced. Devices connected to the UC Merced electronic communications network must comply with the minimum standards for security set by University of California and UC Merced Information Technology policies and procedures. Campus departments, units, or service providers may develop stricter standards for themselves. Devices that do not meet minimum standards for networked host security configurations may be disconnected. Devices that host restricted data as defined in University of California Business and Finance Bulletin IS-3 are required to conform to more rigorous security standards.

This procedure applies to staff, faculty, students, visitors and affiliates.

III. DEFINITIONS

Account: The business record through which service providers authorize access to electronic communications networks under their control.

Administrative Official: A UC Merced employee to whom financial, administrative, or management responsibilities have been delegated, e.g. vice chancellor, provost, dean, department chair, principal investigator, director, or manager.

Authentication: Proof that someone or something is who he, she, or it claims to be.

Electronic Network: A group of two or more computerized communications devices linked together.

Encrypted: Translated into a secret code.

NAT (Network Address Translation): A standard that enables a local-area electronic network to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

Networked Device: A computer, printer, wireless appliance, or other piece of equipment that can connect to and communicate over an electronic network.

Restricted Data: Data whose use is restricted by law, University of California, or UC Merced policy; or data that a Data Proprietor chooses to protect from general access or modification, even if such access may not be prohibited by law, the University of California, or UC Merced policy. Types of restricted data include, but are not limited to, data that identifies or describes an individual and data to which unauthorized access, modification, or loss could seriously or adversely affect UC Merced, its partners, or the public.

Service Provider: A unit, organization, or staff person with responsibility for allowing access to any part of UC Merced's electronic communications systems and services.

SMTP Service: Electronic communication service using "Simple Mail Transfer Protocol", protocol for sending e-mail messages between devices.

System Administrator: An individual responsible for the configuration and maintenance of any device connected to the campus network. This responsibility may occur at the level of a single device (e.g. for an individual using a campus network connection service, such as VPN or WiFi) or for groups of devices (e.g. devices within departments or units, including computer labs) and pertains to system administrators affiliated with the campus, as well as to non-campus personnel serving the campus on an outsourced basis. In the absence of an assigned system administrator, the device user will be considered the system administrator.

Proxy Service: A networked computer that filters requests to other computers.

IV. POLICY TEXT

The University of California, Merced encourages the use of its electronic communications network in support of education, research, and public service. However, this resource is limited and vulnerable to attack. UC Merced therefore reserves the right to deny access to its electronic communications network by devices that do not meet its standards for security.

This policy requires compliance with minimum security standards to help protect not only the individual device, but other devices connected to the electronic communications network. The policy is also intended to prevent exploitation of campus resources by unauthorized individuals.

The policy applies to all devices connected to the campus electronic communications network or using a ucmerced.edu Internet Protocol (IP) address to originate electronic communication. Devices include computers, printers, or other network appliances, as well as hardware connected to the campus network from behind firewalls or Network Address Translation (NAT) systems.

V. PROCEDURES

A. Software Patch Updates

1. Campus networked devices must only run software for which security patches are made available in a timely fashion. All currently available security patches must be applied on a schedule appropriate to the severity of the risk they mitigate.

B. Anti-malware Software

1. For Microsoft Windows or Mac OS X devices for which anti-malware software is available, anti-malware software must be running and up-to-date. In addition, the software must run real-time scanning and/or scan the device regularly.

C. Host-based Firewall Software

1. For Microsoft Windows, Mac OS X, or Linux/Unix devices for which host-based firewall software is available, host-based firewall software must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device. Use of a network-based firewall does not obviate the need for host-based firewalls.

D. Use of Authentication

1. Network services and local (console) device access must require authentication by means of passphrases or other secure authentication mechanisms unless the explicit

purpose of the service/device is to provide unauthenticated access (for example: public web servers or public kiosks) and it can do so without readily allowing it to be used by attackers. Notably, the following network services must require authentication: proxy services, email (SMTP) relays, wireless access points, remote desktop, SSH shell access, and printer administrative interfaces.

2. Simple devices like printers, game consoles, DVR's, media extenders, network-attached storage, and router/firewalls that do not support local authentication are exempt from this requirement if physical access is restricted. This exemption does not extend to network-facing services running on the device.

3. Wireless access points must require strong encryption to associate (such as WPA2), or use a captive portal or some other strong mechanism to keep casual users near the access point from using it to get full access to the campus network. WEP or MAC address restrictions do not meet this requirement.

E. Passphrase Complexity

1. When passphrases are used, they must meet the following complexity specifications:

    a. Passphrases **MUST**:

        i. Contain eight characters ***or more***
        ii. Contain characters from ***two*** of the following ***three*** character classes:
            1. Alphabetic (e.g., a-z, A-Z)
            2. Numeric (i.e. 0-9)
            3. Punctuation and other characters (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

2. Multi-user systems must be configured to enforce these complexity requirements and require that users change any pre-assigned passphrases immediately upon initial access to the account.

3. All default passphrases for access to network-accessible accounts must be changed at time of network connection.

F. No Unencrypted Authentication

1. All network-based authentication must be strongly encrypted. In particular, insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalentsTraffic for one-time password authentication systems (e.g., S/Key, SecureID, Duo Security) is exempted from this encryption requirement.

2. Anonymous FTP servers or other services where authentication credentials are requested but not used are exempt from this requirement.

G. No Unattended Console Sessions

1. Devices must be configured to "lock" or log out and require a user to re-authenticate if left unattended for more than 20 minutes, except in the following cases:

    a. Devices without auto-locking/logoff capability

        i. Devices that do not support a configuration that automatically locks or logs off users after a specified period of time (such as network appliances and consumer electronics) may meet this standard through alternate controls, such as physical access restrictions (e.g., appliance stored in a locked office).

    b. Devices which are physically secured

        i. Devices kept in a physically secured space not accessible by unauthorized users are exempt from this standard.

    c. Kiosks and other public-use devices are exempt from this requirement.

H. No Unnecessary Services

1. If a network service is not necessary for the intended purpose or operation of the device, that service must not be running.

I. Privileged Accounts

1. Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrator activities. A secure mechanism to escalate privileges (e.g., via User Account Control or via sudo) with a standard account is acceptable to meet this requirement. Network services must run under accounts assigned the minimum necessary privileges.

    a. The following cases are exempt from this requirement:

        i. Devices that do not support separation of privileges

        ii. Devices that do not provide separate facilities for privileged or unprivileged access (e.g., some network appliances and printers with embedded operating systems) are exempt from this requirement.

VI. RESPONSIBILITIES

1. **Campus Administrative Officials**

    a. Ensure that devices connected to the electronic communications network from their department or unit are supported by an administrator or user with the ability to maintain minimum security standards.

2. **System Administrators or anyone functioning as a System Administrator**

    a. Ensure compliance with minimum standards for security as set forth in the Procedures section below.

3. **Information Technology**

    a. Provides direction, planning, and guidance about information security.

    b. Develops and reviews campus-wide information security policy and procedures.

    c. Writes minimum security standards for networked devices.

    d. Approves exceptions to minimum security standards.

    e. Works with the campus community to protect computers and the campus network infrastructure from electronic attack.

    f. When necessary, blocks access to UC Merced's electronic communications network in accordance with the UC Merced Acceptable Use Policy.

4. **Departments, Units, and Individuals**

    a. Use devices that comply with the minimum standards set forth in this policy.
    b. Function as the system administrator in the absence of an assigned system administrator.

VII. POLICY OR PROCEDURE REVISION HISTORY

APPENDICES

Not Applicable