

UC Merced Policy on the Management of Network Name Spaces and Infrastructure

(Approved 9/14/2004)

I. INTRODUCTION

The University network is a shared resource used to support the University's mission of teaching, research, and public service, and to conduct the University's business. It is accordingly necessary to manage the network in such a manner as to ensure its availability for these purposes, and also, to the extent that elements of the network or services running on it interact with external networks, ensure conformance with responsible behaviors (in the sense of network protocol usage, defenses against hacking, etc.). Additionally, the assignment of published network names to network resources must be consistent with University communications standards and strategies.

The UC Merced Appropriate Use Policy primarily addresses responsible and appropriate use of the network and network services by individuals. The Policy on the Management of Network Name Spaces and Infrastructure primarily addresses the provisioning of network services and the allocation of related responsibilities to ensure the availability of the network and network services now and in the future.

The Policy on the Management of Network Name Spaces and Infrastructure in many cases assigns prerogatives to the Information Technology department (hereinafter referred to as "IT"). The impetus for this is the need to ensure the interoperability of the various network elements and services, the desire to minimize the time needed to diagnose and resolve network problems, and the need to ensure our ability to evolve the network infrastructure to meet our needs and to stay in step with changes in external networks (for example, migration from Internet Protocol v4 to Internet Protocol v6).

II. AFFECTED AREAS

A. **Domain Names**

1. All official University services that are advertised and/or accessible via domain name services must use domain names that are owned or effectively controlled by UC Merced.
2. All such domain names must refer to sub-domains of **ucmerced.edu**, except where special permission is granted.
3. Special permission will be granted only in cases where UC Merced is acting as host for a non-UC Merced organization or function.
4. IT will coordinate the assignment of sub-domain names within the **ucmerced.edu** domain, delegating the assignment of additional naming within sub-domains as appropriate.
5. Domain Name Services (DNS) will be furnished by IT, except where special permission is granted to a unit or group to run their own Domain Name Server.
6. Such permission is intended to be accorded when there is a reasonable, demonstrated need to run such a service, when the technology level of the platform providing the service is deemed to be adequate, and when the staff responsible for running the service has the appropriate skills, and is available to assist in problem determination on a 7/24 basis.
7. Domain names shall not contain words or expressions that reasonable people may believe to be potentially offensive to any group.

B. **Universal Resource Locators (URLs)**

1. All official University activities that are web-based must be conducted on sites whose domain names are owned or effectively controlled by UC Merced.
2. All official University activities that are web-based must be conducted on sub-domains of **ucmerced.edu**, except where special permission is granted.
3. Special permission will be granted only in cases where UC Merced is acting as host for a non-UC Merced organization or function.
4. For the University web site, IT will coordinate the assignment of qualifiers that occur following the domain name within the URL (i.e., <http://www.ucmerced.edu/qualifier1/qualifier2/...>), delegating the assignment of additional qualifiers as appropriate.

5. URLs shall not contain words or expressions that reasonable people may believe to be potentially offensive to any group.

C. Internet Protocol (IP) Addressing

1. All computers and other devices directly connected to the University network must use IP addresses that are assigned to the University and managed by IT or an authorized delegate.
2. IT will allocate portions of the University IP address space to buildings, organizational units, logical entities, or otherwise, as it deems appropriate, to the end of providing for availability, management, scalability, and future expansion.
3. IT will delegate the management of portions of the University IP address space to groups or organizational units that have the need and ability to do so.
4. IT will operate all Dynamic Host Configuration Protocol (DHCP) servers except when special permission is granted to others to do so.
5. Such permission is intended to be accorded when there is a reasonable, demonstrated need to run such a service, when the technology level of the platform providing the service is deemed to be adequate, and when the staff responsible for running the service has the appropriate skills, and is available to assist in problem determination on a 7/24 basis.

D. Routers and Switches

1. Routers and Layer 3 switches will be deployed and managed exclusively by IT.
2. Layer 2 switches will normally be deployed and managed by IT, but management may be delegated to other units when appropriate.
3. Even when financed outside of IT, procurement of network equipment will be the responsibility of IT, in accordance with established campus standards and negotiated vendor contracts.

E. Wireless Devices

1. Per the Policy Governing Wireless Networking and Other Uses of the Radio Frequency Spectrum at UC Merced, IT is responsible for deploying and operating wireless networking on campus, and for publishing guidelines on the use of equipment that may interfere with the operation of wireless networking.
2. Although the actual details are available in the aforementioned policy, the thrust of that policy is that IT will delegate the right to install and operate wireless access points to other units only under very limited circumstances.

F. Authentication and Security

1. IT has over-arching responsibility for ensuring the security of the wired and wireless aspects of the campus network, including the connection of remote devices and networks by dial-up or other telecommunications technologies.
2. IT will allow access only through IP ports and protocols consistent with assignment and usage as specified and/or recognized by the Internet governing bodies and general usage, and known not to be unusually vulnerable to external threats. IT will publish the list of usable ports and work on a good faith basis to enable additional ports when requested.
3. IT may temporarily, and before giving notice, block normally usable ports under the existence or threat of a known attack until protective measures are taken on computers and/or network devices internal to the campus network.
4. IT has the right to impose reasonable authentication requirements on devices connected to the campus wired and/or wireless networks, and to restrict or manage the connection of remote devices.

G. Network Monitoring

The provisions in this section are subject to the individual privacy provisions mandated in the University of California Electronic Communications Policy and the UC Merced Acceptable Use Policy.

1. IT has the right to run software which inspects network traffic and/or device configurations to:
 - a) analyze network performance and resource utilization,
 - b) perform intrusion detection,
 - c) detect and/or audit security vulnerabilities on servers and other computers,
 - d) ascertain the presence of appropriate virus detection software on computers,
 - e) detect the active execution of hacking or virus/worm distribution programs.

2. Analysis of packets captured to study performance, utilization, and similar activities will be performed only in the aggregate and will not include human inspection of individuals' data.
3. The capture and analysis of individual packets may be necessary to resolve specific problems or security exposures. In this case, only packet types needed to perform problem determination will be inspected, and affected users will be notified prior to such activities, always assuming that they can be identified before the fact. Inspection of packet contents shall be limited to those fields directly relevant to problem determination.

III. ENFORCEMENT

1. In the case of immediate danger to the availability of the campus network or in any similar situation deemed to present a high risk, IT may disconnect devices from the campus network without prior notice. However, in such cases, IT should make a good faith effort to contact the responsible and/or affected parties before such action is taken, and, if unsuccessful, continue such efforts after action has been taken.
2. In other cases where undue vulnerabilities and/or violations of this Policy are detected, disconnection of devices shall occur only after multiple notifications have been issued to the responsible parties and only after a reasonable amount of time has passed that would allow for vulnerabilities to be corrected.

IV. DISPUTE RESOLUTION

The Provost and Executive Vice Chancellor shall have the ultimate authority in resolving disputes relating to all aspects of this Policy, including, but not limited to, the use of names, address spaces, network devices, and network services.