



---

**UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL**

TITLE:	DNS / DHCP Policy	REFERENCE:	New
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	New
APPROVER:	David Ertel	VERSION:	1
	Interim Senior Vice President	EFFECTIVE:	March 1, 2017
	Business and Finance		

---

**I. PURPOSE:**

The domain name system (DNS) maps a computer's canonical name (*i.e.*, [www.miami.edu](http://www.miami.edu)), to its assigned IP address. This enables an individual to access a network device's content or services by name instead of entering the IP address. In an IP environment, the DHCP server assigns the IP address to the computer or device.

The purpose of this policy is to establish a basis for centralized management of the University of Miami (University) domain names and supporting DNS and DHCP network services. The centralized management of these services is a critical component to University operations. Domain names communicate the University's identity and image to the public and its supporting DNS/DHCP services requires consistency to ensure business continuity throughout all campuses.

**II. SCOPE:**

This policy applies to University employees, faculty, students, contractors, guests, consultants, vendors, and other non-University employees seeking domain name requests or implementation of DNS/DHCP services and the network devices used to deliver these services.

**III. POLICY:**

University of Miami Information Technology (Central IT) is responsible for the maintenance, operation and security of the network infrastructure and its services. In fulfilling this role, it is the policy of the University that domain name systems and the DHCP services provided by the University network will be centrally managed for consistent and secure administration.

**DEFINITIONS:**

**DHCP:** Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

**DNS:** Domain Name System. A DNS server provides domain name resolution services to Web hosts and clients on an IP-based network.

**Hostname:** The name assigned to a device (host) on a network. The hostname distinguishes one device from another on a specific network or over the Internet.

**IP Address:** Internet Protocol address. A unique address that identifies a device on the internet or a local network.

**Static IP:** A permanent IP address assigned to a device on a network.

**Subdomain:** A sub-domain is a logical representation of a top-level domain subset, usually taking the form of organizationalunit.miami.edu.

**Top level domain:** The University of Miami uses the top-level domain of miami.edu. An example of a non-miami.edu top level domain that may be acquired for business purposes is sylvestor.org.

#### **IV. PROCEDURE:**

##### **A. Domain Name Registration**

1. The approval and registration of top-level domain names for the University will be maintained by UM Communications.
2. Requests for domain names must be submitted to [webmaster@miami.edu](mailto:webmaster@miami.edu) for approval.
3. Top-level domain names that are acquired to protect University interests and do not represent services, must not resolve to any service, or redirect to a hostname or subdomain within the University top-level domain.
4. Approved domain and subdomain names along with the corresponding associated college or administrative unit must be submitted to Central IT.
5. Subdomains or hostnames reflect the University of Miami. Name selections must be in good taste, represent the purpose of a system and must be approved at the departmental level. Central IT has the right to refuse a sub-domain or hostname if deemed inappropriate or causes confusion about the purpose of a system.

##### **B. Domain and Sub-Domain Hosting**

1. University domain names and subdomains must be hosted on University of Miami servers only.
2. Domains and subdomains will not be hosted for non-University related purposes.

##### **C. DNS Administration**

1. Central IT is responsible for maintaining University DNS records.
2. Central IT will assign and register IP addresses that map to a domain or subdomain.
3. Domain names administered should have reverse canonical name mappings.
4. Requests and changes to DNS records must be submitted to UMIT Helpdesk.

##### **D. DHCP Management**

1. Central IT will manage IP address blocks, subnets, DHCP address assignments, and lease duration for hosts that connect to the University network.
2. Requests for static IP(s) and IP address block(s) must be submitted to UMIT Helpdesk. Static IP addresses will be assigned in limited cases and require a specific need.

3. Departmental IT staff will only register static IPs created in the subnets allocated for their department.
4. Static IP address assignments will be reviewed annually to verify continued need.

**E. Rogue DHCP Servers**

1. Wired and wireless network devices that provide unapproved DNS/DHCP services will be detected as rogue.
2. Central IT reserves the right to remove or isolate rogue equipment from the University network, as an unauthorized addition or change may compromise the availability, performance, security and reliability of the University network.

**F. Violations**

Violations of this policy will be addressed by the procedure applicable to the individual.