CORNELL UNIVERSITY
POLICY LIBRARY

Network Registry

POLICY 5.7

Volume 5, Information Technologies

Chapter 7, Network Registry

Responsible Executive: Vice President for Information Technologies

Responsible Office: Office of Information Technologies

Issued: June 1, 2004

POLICY STATEMENT

Cornell University requires network administrators or users to register all devices (including wireless hubs and switches) connected to the network in a continuously updated central CIT network registry service. At a minimum, the required information maintained in this registry must include MAC address and IP address, if static, as well as the network electronic identifier (netid) of the primary user or the person responsible for the administration of the device.

REASON FOR POLICY

To enhance the maintenance and security of the university network, and to alleviate potential legal risk, the university supports the creation of a central registry of devices connected to the university network.

ENTITIES AFFECTED BY THIS POLICY

Endowed Ithaca and Contract Colleges of the University, (Excluding the Joan and Sanford I. Weill Medical College)

WHO SHOULD READ THIS POLICY

- All Members of the University Community

WEBSITE ADDRESS FOR THIS POLICY*

http://www.policy.cornell.edu/IT_policies.cfm

Policy 5.7
Network Registry

CONTENTS

Policy Statement	**1**
Reason for Policy	**1**
Entities Affected by this Policy	**1**
Who Should Read this Policy	**1**
Website Address for this Policy	**1**
Related Documents	**3**
Contacts	**3**
Definitions	**4**
Procedures	**5**
Introduction	5
Users or Systems Administrators	5
Network Administrators	5
Cornell Information Technologies	6
Related Violations	6
Reporting Violations	6
Responsibilities	**7**
Index	**8**

Policy 5.7
Network Registry

RELATED DOCUMENTS

Table 1
Related Documents

University Documents	Other Documents
Cornell University Policy Regarding Abuse of Computers and Network Systems	
University Policy 4.12, Data Stewardship and Custodianship	
University Policy 5.1, Responsible Use of Electronic Communication	
University Policy 5.4.1, Security of Information Technology Resources	
University Policy 5.4.2, Security Incident Reporting	

CONTACTS

Direct any general questions about University Policy 5.7, Network Registry, to your unit's administrative office. If you have questions about specific issues, call the following offices:

Table 2
Contacts

Subject	Contact	Telephone	Email/Web Address
Policy Clarification and Interpretation	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Security of Network Systems	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/

DEFINITIONS

These definitions apply to these terms as they are used in this policy.

Information Technology Device	Any device involved with the processing, storage, or forwarding of information making use of the Cornell information technology infrastructure or attached to the Cornell network. These devices include, but are not limited to, laptop computers, desktop computers, servers, and network devices such as routers or switches, and printers.
IP Address	Internet Protocol Address. A unique number associated with a device used for the routing of traffic across the Internet or another network.
MAC Address	Media Access Control Address. A unique number assigned to the hardware within a device used for mapping its IP address.
Network Administrator	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device, including network registration, on a separated subnet.
Separated Subnet	A subnet within the university's network residing behind a single port gateway, firewall, or separately routed network.
Subnet	A section of the university's distributed network.
Systems Administrator	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device, including network registration, on a subnet.
User	An individual who uses an information technology device.

Policy 5.7
Network Registry

PROCEDURES

Introduction

Cornell Information Technologies (CIT) is charged with creating a central network registry service. This service maintains a current record of all devices connected to the Cornell University network through a continually updated database. This policy extends to wireless communications.

Users and Systems Administrators

1. The CIT central network registry service will automatically generate a registration page when a user or systems administrator connects an information technology device to the CIT-managed network. The user or systems administrator must complete this page before the device is operated on the network. The page requires the following information from members of the Cornell community:

- MAC address;
- IP address, if static;
- the network electronic identifier (netid) of the primary user of the device, or, if a shared device, the netid of the person responsible for the administration of the device.

2. If the user or systems administrator does not receive a registration page, (e.g., because the device is on a separated subnet, because the device is a printer, or for any other reason) he or she must contact his or her network administrator to register the device.

u **Note:** Nothing in this policy shall be construed to impede the development of a guest registry system.

Network Administrators

1. Network administrators are required to register all devices connected to networks under their domains for which individual users or systems administrators, for whatever reason, have not themselves registered, to http://networkregistry.cornell.edu.

☐ **Note:** Model and serial numbers are required for devices that predate the MAC address system.

2. Network administrators of separated subnets, in addition to the actions in 1, above, must supply the CIT central network registry service with logs of MAC addresses of devices that connect to their networks to http://networkregistry.cornell.edu.

☐ **Note:** Users who connect to internal modem pools or virtual private networks (VPNs) that require authentication are exempt from the procedures

PROCEDURES, CONTINUED

of this policy because authentication provides the necessary identification of both device and user.

Cornell Information Technologies (CIT)

CIT will provide the technical tools necessary to access the central network registry service to network administrators who manage subnets. For more information, go to http://networkregistry.cornell.edu.

Related Violations

Anyone who changes a MAC address, IP address, or netid with the intention of disguising or forging his or her identity may be in violation of University Policy 5.1, Responsible Use.

Reporting Violations

Report all suspected violations of this policy to the Director of IT Security, at security@cornell.edu.

RESPONSIBILITIES

The major responsibilities each party has in connection with University Policy 5.7, Network Registry, are:

Cornell Information Technologies	Create and manage a central network registry service. Provide the technical tools necessary to access the central network registry service to network administrators who manage subnets.
Director of IT Security	Receive reports of and investigate suspected violations.
Network Administrator	Ensure that all devices attached to their subnets are registered in the CIT Central Network Registry Service. Maintain and monitor registration. For those who manage separated subnets, supply a log of MAC addresses attached to their networks to networkregistry@cornell.edu.
System Administrator	Complete the CIT central network registry service registration page for users who are unable to do so.
User	Complete the CIT central network registry service registration page or contact the network or system administrator to request registration.