COLUMBIA UNIVERSITY
NETWORK PROTECTION POLICY

Published: October 2013
Revised: November 2014,
September 2016, July 2019

I. Introduction

The secure management of the University Network (as such term is defined in the Columbia University Information Security Charter (the "Charter") http://policylibrary.columbia.edu/information-security-charter, which may span organizational boundaries, requires the careful consideration of the flow of information and the regulatory requirements regarding monitoring and protection of Networks. The University requires that all Network, communications and telecommunications related equipment and devices, including cabling, be installed and maintained by CUIT or CUIMC IT, either alone or in collaboration with NewYork-Presbyterian Hospital Information Technology.

Capitalized terms used herein without definition are defined in the Charter**.**

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy replaces the University Network and Communications Equipment Policy, dated June 2011.

III. Policy Text

This Policy applies to all communications cabling, equipment and infrastructure devices, including but not limited to the following: telecommunications switches, data networking switches and routers, wireless access points, cellular distributed antenna systems, cellular repeaters and/or bi-directional amplifiers, cellular macro sites, cable and satellite television reception and distribution equipment.

A. Standard Requirements

1. The following equipment must be installed and maintained by CUIT or CUIMC IT:

    - Communications cabling, including any permanent cabling and/or cabling between workspaces and rooms intended to be used for voice and data networking or other communications;
    - Routers on the University Network that serve to segment the Network;
    - Communications switches and hubs (e.g., Ethernet switches) on the University Network;
    - Wireless Access Point (WAPs) and other wireless devices that provide access to, or bridge, the University Network;
    - Telecommunications equipment (e.g., PBXes, VOIP systems, etc.);

- Cellular telephone (voice and data) communications infrastructure cabling, antennas, and equipment; and
- Cable and satellite television infrastructure cabling, antennas and equipment.

2. All Network enabled devices connected to the University Network (other than Network enabled devices connected to the CUIMC Network) must use (a) the DHCP to configure Network IP addresses and (b) the DNS protocol for Server information. Network enabled devices connected to the CUIMC Network must adhere to CUIMC's Network and security procedures.
3. CUIT and CUIMC IT staff implement the appropriate logging and monitoring of Networks in accordance with the Columbia University Information Resource Access Control and Log Management Policy http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy**.**
4. Standard protections are established by the applicable Information Security Office and implemented by CUIT or CUIMC IT staff to safeguard the confidentiality and integrity of University information passing over public and wireless Networks.

B. Bandwidth Quotas

To maintain Network performance, CUIT has implemented an automated Network bandwidth quota system. Individual computers may be limited in either the inbound or outbound direction. Limits are imposed only on off-campus traffic to or from the Internet. Traffic on the University's internal Network and on Internet2 is not restricted in any way.

The parameters of this system may be changed without prior notice in order to ensure proper functioning of the Network for the University community.

An exception to the Internet bandwidth limitations may be granted for Servers used for legitimate University business through the use of the **Network Quota Exception Request** https://www1.columbia.edu/sec/acis/support/consultant/staffonly/bandwidth-exception.html

See **Bandwidth Quotas and Network Performance** http://www.columbia.edu/cgi-bin/acis/networks/quota/netquota.pl for more information on bandwidth quotas.

C. Waivers and Exceptions

Any Executive Manager may request that a Network or communications infrastructure that is not maintained by CUIT or CUIMC IT be granted a waiver of the provisions of this Policy by the applicable Information Security Office. Such a waiver may only be granted if such Officer determines that there are compensating controls in place to address all major information security risks.

IV. Cross References to Related Policies and Other Documentation

The Information Security Policies and certain additional documentation are listed in Appendix A hereto.

Appendix A

Related Policies and Other Documentation

Bandwidth Quotas and Network Performance
http://www.columbia.edu/cgi-bin/acis/networks/quota/netquota.pl

Information Resource Access Control and Log Management Policy
http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter

Network Quota Exception Request
https://www1.columbia.edu/sec/acis/support/consultant/staffonly/bandwidth-exception.html