Network and Communications Equipment Policy

Policy Statement
Columbia University requires that all network, communications, and telecommunications related equipment and devices, including cabling, be installed and maintained by the Columbia University Information Technology (CUIT) department, by the Columbia University Medical Center Information Technology (CUMC IT) department, or by CUMC IT in collaboration with the NY Presbyterian Hospital Information Technology (NYPH IT) department.

Existing network or communications infrastructure, that has already been installed and maintained elsewhere as of the effective date of this policy, may be retained with the approval of CUIT or CUMC IT.

The University reserves the right to modify or amend this policy and to limit or restrict the use of its electronic information resources at its sole discretion.

Reason for the Policy
Columbia University’s network and computing technology provides information, data, and communication services. CUIT and CUMC IT (collaborating with NYPH IT) are responsible for maintaining and supporting the entire Columbia University campus network infrastructure, and overall operations and security of the University’s networks. To ensure proper operation, support, and security of the University’s networks, CUIT and CUMC IT must maintain the ability to configure and monitor all network, communications, and telecommunications related equipment and devices.

Primary Guidance to Which This Policy Responds
This policy is established under the provisions of Columbia University’s Information Technology, Security and Policy Program.

Responsible University Office & Officer
The office of Columbia University Information Technology is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Technologist is the responsible officer.

Revision History
This policy was established in April 2011.

Who is Governed by This Policy
This policy applies to all individuals who access, use, or control University electronic information resources. Those individuals covered include, but are not limited to staff, faculty, students, those working on behalf of the University, guests, tenants, visitors, and individuals authorized by affiliated institutions and organizations.
Who Should Know This Policy
All individuals governed by this policy should be familiar with it.

Exclusions & Special Situations
Existing network or communications infrastructure, that has already been installed and maintained elsewhere as of the effective date of this policy, may be retained with the written approval of CUIT or CUMC IT. Where such infrastructure exists, description and request to retain with rationale should be forwarded to CUIT or CUMC IT via the Columbia University IT Leadership Council member responsible for the respective school or department. If approved, the exception will be subject to annual review.

Exceptions for any future infrastructure installations must be requested and sent to CUIT or CUMC IT by a University Dean or Vice President. Exception requests will be considered only for compelling business or research need that cannot be met by CUIT or CUMC IT. If approved, the exception will be subject to annual review.

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.

Any and all communications cabling shall be installed and maintained by CUIT or CUMC IT. This includes any permanent cabling and/or cabling between workspaces and rooms intended to be used for voice and data networking or other communications. Structured cabling systems serve to hinder physical compromises of cabling through the use of enclosed pathways and secure cable termination facilities. Columbia University uses modern cabling systems and adheres to installation specifications to ensure maximum performance and minimum disruption due to compromised system integrity. Columbia University designs cabling configuration to maximize performance and reliability.

All routers on the campus network shall be installed and maintained by CUIT or CUMC IT. Routers serve to segment networks and enforce security policies. Routers may also obscure network devices that are part of the campus network. Therefore, it is necessary for CUIT and CUMC IT to maintain routers because of inherent responsibility to provide overall network operation, support, and security.

All network communications switches (e.g., Ethernet switches) on the campus network shall be installed and maintained by CUIT or CUMC IT. Switches serve to move communications traffic between various network endpoints while segmenting networks and enforcing security policies. Many switches provide a means to tap into communications traffic, which provides a malicious user with a potential method to compromise data security.

All Wireless Access Point (WAPs) and other non-client devices (e.g., Repeaters) on the campus network shall be installed and maintained by CUIT or CUMC IT. WAPs serve to move
communications traffic between various network endpoints while segmenting networks and enforcing security policies. Many WAPs combine features of routers and switches, and the shared nature of wireless communications makes them inherently insecure without proper configuration and use of strong encryption. Due to the shared nature of wireless communications, deployment of WAPs must also be coordinated in order to prevent harmful interference.

All telecommunications switches (e.g., PBXes) on the campus shall be installed and maintained by CUIT or CUMC IT. Telecommunications switches serve to move voice communications traffic between various network endpoints while enforcing security policies. Many telecommunications switches provide a means to tap into communications traffic, which provides a malicious user with a potential method to compromise data security. Telecommunications switches are also subject to regulatory requirements regarding emergency calling and law enforcement communications intercepts.

All cellular telephone (voice and data) communications infrastructure cabling, antennas, and equipment shall be installed and maintained by CUIT or CUMC IT. The cellular infrastructure (e.g., distributed antenna systems, bi-directional amplifiers) assures reliable mobile voice and data communications and is subject to regulatory requirements including emergency calling and emergency location services. The University relies on cellular services for emergency notification (“reverse 911”) of the University population. Cellular wireless services must be coordinated so as not to cause or be subject to harmful interference and to comply with applicable regulations.

All cable and satellite television infrastructure cabling, antennas and equipment shall be installed and maintained by CUIT or CUMC IT. Columbia University standards ensure that antennas, cables and equipment installed for cable and satellite television are installed safely and without causing damage or unsightly alterations to the University’s buildings.

Central administration of all campus routers, switches, WAPs and other non-client devices ensures proper implementation of configurations and security policies and minimizes the risk of data security compromise.

Columbia University uses enterprise-grade routers, switches, and wireless systems that provide performance, scalability, and availability. CUIT and CUMC IT operations staff continuously monitors the utilization and health of all network components and security incidents on a 24x7x365 basis, and respond to address problems and abnormal situations.

**Enforcement**

Violations of these policies may result in the immediate suspension of network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations will be referred directly to the appropriate University or outside authorities. Unauthorized use of University computing facilities is strictly prohibited. The penalties may be as severe as suspension or dismissal from the University and/or criminal prosecution.

**Definitions**
Data is a stored collection of information that may include alphanumerics, words, sounds, symbols, or images.

Electronic Information Resources include data, networks, computers, and other devices that store or display data, communications devices, and software used on such devices.

Contacts
For questions or comments:
Columbia University Information Technology
   Web: http://www.columbia.edu/cuit/support/
   Email: askcuit@columbia.edu
   Telephone: 212-854-1919

Cross References to Related Policies
For IT Security Policies, see the University Administrative Policy Library, CU Information Technology section:

http://policylibrary.columbia.edu/node_browser/nodes_by_category/term/7