

The City University of New York

IT Security Procedures - Wireless Network Security, #2009-01

Issued by: Brian Cohen, Associate Vice Chancellor and Chief Information Officer

Effective date: 12/01/2009, Last revision date: 11/20/2009

Questions, comments, revisions: Computing & Information Services Information Security, security.cuny.edu

Scope: Wireless network facilities managed by the University or Colleges.

Related Policies and Procedures (under Info Security Policies at security.cuny.edu):

Policy on Acceptable Use of Computer Resources

IT Security Procedures

1. Requests to install new wireless networks or change existing wireless networks must be in writing and will be subject to approval by the College CIO or, for Central Office departments, the University CIO. The College CIO or, for Central Office departments, University CIO will routinely monitor for unauthorized (rogue) wireless networks and such rogue networks must be disconnected when discovered.
2. New wireless networks or modifications to existing wireless networks will be subject to a risk assessment to determine if such wireless networks comply with this Procedure, the University Acceptable Use of Computer Resources Policy, University IT Security Procedures, and College policies and procedures.
3. All wireless networks must require the use of routine monitoring and preventative techniques to minimize risks of unauthorized intrusion attempts. Techniques may include, but are not limited to, end-point integrity checks before allowing wireless connected devices to authenticate to University and College applications, wireless network behavioral analysis, and log data analysis.
4. Wireless visitor access and devices failing an end-point integrity check must be redirected to the Internet over a private virtual LAN that does not route to any other subnet(s) of the University or College network infrastructure.
5. University and College web applications, if non-public University data is transmitted, must use the secure and encrypted protocol https.
6. Wireless usage logs must be retained consistent with the University Records Retention and Disposition Schedule (www.cuny.edu/policy/text/toc/rrs) and include Media Access Control address, IP address, time stamp and user ID to enable tracing of security incidents and the source of copyright infringement claims and other security incidents.
7. Signal strength and containment of the wireless signal must be engineered to minimize the wireless signal accessibility outside the bounds of the College's business and community mission.