Wireless Security Policy

The Policy

Wireless devices or networks used to access, store, process, or transmit City of New York information or access Citynet must be implemented in a secure manner.

Background

Wireless devices and networks enable un-tethered communications to mobile users. Improperly installed, configured or managed wireless technology presents a significant risk to the confidentiality of information. Wireless network security refers to the protection of wireless network hardware, software, and the information contained in them from threats caused by the inherent vulnerabilities in the technology and its implementation.

Scope

This policy applies to all wireless devices, networks, services, and technologies used to access, store, process or transmit city information or connect to Citynet. The term “wireless” refers to any technology that does not use cables.

Wireless includes radio frequency (i.e. satellite, microwave, radio) and optical (i.e. infrared) technologies.

Wireless networks include both wireless local area networks (WLANs) and wireless wide area networks.

Wireless devices are any end-user device that uses wireless technology to communicate. These include but are not limited to: Personal Digital Assistants (PDAs), cellular phones, laptop computers, printers, wireless keyboards, wireless mice or trackballs, and bar code scanners

Wireless Network Nodes are network elements that terminate one end of the wireless communication. That communication may be between a wireless device and a wireless network element or between two wireless network elements.

Wireless Bridges are wireless transceivers used to connect two or more remote networks. They are typically used to provide campus building-to-building wireless connectivity

Appropriate Use

1) Wireless technology may be used to access, store, process or transmit City of New York business and connect to Citynet’s infrastructure provided that it conforms to all applicable DoITT Information Security Policies including but not limited to this policy.
2) Wireless devices may not be used to gain or attempt to gain unauthorized access to any network. This includes accessing Citynet, external non-city networks and the internet where the user has not been granted access.
3) Only approved services and applications may be used with wireless devices.
4) Any planned wireless connection(s) must be reviewed and approved in advance of installation by the local agency including the agency CISO. If the wireless connection(s) provide access to Citynet, or a network connected to Citynet, then

approval must include DoITT.

5) The Wireless network must have a disaster recovery plan if required based on business function of the applications running on the network.

Access Control

6) Access to the city's networking and computing infrastructure via a wireless connection is considered remote access and must utilize strong authentication and encryption.
7) The Agency must use the current City of New York wireless standard at the time of the implementation of their wireless system.
8) Appropriate encryption utilizing approved ciphers must be used.

Risk Assessment

The agency CISO should employ security measures commensurate with the risk associated with the wireless network. If the network is used for transmission of business sensitive material, classified communications or supports City critical services the risk of loss in the event of an attack on the wireless network, or loss of service can be extensive.

9) Due to the ever changing threats and vulnerabilities, risk assessments should be conducted on a periodic basis no less than annually to provide an accurate picture of the total risk to the organization.
10) A risk assessment should be performed to ensure the capabilities of protection for the technologies utilized. A risk assessment should include but not be limited to; identifying data sensitivity, network vulnerabilities, and critical services. The focus should be to identify potential threats and vulnerabilities.

Authentication

11) All users of WLANs are required to authenticate before being allowed to access the network.

Document Revision History

Date	Description
June 16, 2011	**Version 1.2** Updated header with new NYC logo and added this revision history table to the document.