IT Policy 11.01

Information Technology

Subject: **WIRELESS ACCESS POLICY**

Scope: **ALL COUNTY, LIBRARY, LODGE AND CONTRACT EMPLOYEES**

Issued: **September 25, 2023**

Revised:

Purpose

The purpose of this policy is to outline the secure and appropriate use and configuration of Wireless Networks.

Definitions

“Corporate Network” is the Wired or Wireless network provisioned by Middlesex County ITS which can allow authorized access to Corporate Information.

“Corporate Information” is any information, files, or communications which could be considered sensitive, privileged, or confidential, stored within ITS Assets owned by Middlesex County.

“Guest Network” is a dedicated Wired or Wireless Network which allows users access to the Internet or specific designated resources, while restricting access to Corporate Networks or Corporate Information.

"ITS" means Information Technology Services.

"Middlesex County ITS" is the department at Middlesex County responsible for procurement, maintenance, and support of Information Systems

“Network Device(s)” are physical devices capable of connecting multiple devices together on a wired or wireless network.

“Smart Device” are any device that can connect to a wired or wireless network to perform a task or automation such as a thermostat, fridge, sprinkler, lightbulbs, HVAC controller, door lock, or temperature sensor.

“Wireless Access Point(s)” are physical devices capable of broadcasting a signal for other devices to use for connecting to a Wireless Network.

"Wired Network(s)" are any network which uses a physical medium such as wires or cables to connect devices together for the purposes of transferring information.

"Wireless Network(s)" are networks which provide services to devices through the air without requiring a physical connection to a Wired Network.

"Virtual Private Network (VPN)" is a method in which an approved staff member can securely access Corporate Information from a remote location, using approved software, hardware, or a combination thereof.

Policy

a) Wireless Networks supported by Middlesex County ITS shall be configured in a manner which ensures reliable operation and secures data and information.

b) Wireless Networks shall be segmented between external guest and internal networks to ensure the security and integrity of internal data.

c) Non-Middlesex County devices shall not be connected to the Middlesex County's internal Corporate Network.

d) Wireless access points or Network Devices with wireless capability are not to be connected to Middlesex County networks unless approved by Middlesex County ITS.

e) Staff and guests shall not use Middlesex County Wireless Networks in a manner which negatively impacts the performance of these networks.

f) Staff shall not share or make public wireless network passwords to any staff or guests which have not expressly been granted access to the Wireless Network.

Procedures

1. Configuration

The following procedures and practices shall be implemented to reduce risks related to wireless networks.

a) Wireless Networks shall be segmented between external guest and internal (Corporate) networks.

b) User access to Corporate Wireless Networks shall be restricted to authorized personnel and devices.

c) Wireless Networks may be configured in a manner that automatically disconnects wireless devices after a predetermined period, requiring these devices to be reconnected to the Wireless Network.

d) Perimeter firewalls shall be implemented and configured by Middlesex County ITS to restrict unauthorized access while connected to a Wireless network.

e) Wireless security protocols shall be used that are of the highest available encryption where possible.

f) Audit logs shall be collected for the purposes of determining performance and troubleshooting Middlesex County Wireless Networks. Additional information may be gathered as defined in the Electronic Monitoring Policy (HR Policy 1.17).

2. Unapproved device connections

a) Wireless Access Points or Network Devices with wireless capability shall not be connected to Middlesex County Guest or Corporate Networks unless approved and installed by Middlesex County ITS or a contractor authorized by Middlesex County ITS.

b) Wireless devices which have not been approved by Middlesex County ITS shall not be connected to Middlesex County's Corporate Network. This includes but is not limited to: Smart Devices, wireless printers, security cameras, and point of sale (POS) terminals.

3. Transmission of sensitive or confidential documents on a public / guest network

a) Middlesex County staff shall not use any public or guest network to transmit documents or information which could be considered sensitive or private in nature unless connected through a Middlesex County ITS provided Virtual Private Network (VPN) connection.
b) Where possible, staff are encouraged to find an alternate method for transferring these documents or information, including a secured hard-wired connection or workstation.

4. Large file transfers

a) Both Corporate and Guest Wireless Networks may be limited in a manner to prevent staff and visitors from impeding on the usage of others.
b) Users wishing to transfer a large volume of files or data should find alternate means to do so, including a hard-wired connection/workstation, or using an approved physical medium such as a USB flash drive or key.
c) Devices connected to Corporate Wireless Network or external (public / guest) networks which are consuming a large number of resources may be restricted from accessing wireless networks.

5. Compliance

Middlesex County ITS enforces this Policy and related standards. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS.