



State of North Carolina
Department of Public Safety
POLICIES & PROCEDURES

INFORMATION TECHNOLOGY

Division: ADMINISTRATION
Chapter: INFORMATION
TECHNOLOGY
Policy: WIRELESS
ACCESS
Issue Date: JANUARY 26, 2013
Revised:

I. PURPOSE

To provide guidance regarding the secure installation and use of wireless access points and wireless devices within Department of Public Safety facilities.

II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office (Statewide Information Security Manual (020104, 030101, 060101, 090301); G.S. § 147-33.110; G.S. § 148-23.2).

III. POLICY

1. Access Points

- a. Requests for wireless access points shall be documented, by the appropriate manager, in a written request to the MIS section.
- b. Prior to purchasing a wireless access point, the DPS Information Security Office or qualified third party shall perform a risk assessment of the proposed site. Sites must meet the minimum security requirements established by the DPS Information Security Office or have sufficient compensating internal controls. Compensating internal controls must be approved by the Information Security Office.
- c. Subsequent to the risk assessment, a wireless access point may only be purchased with written authorization from the MIS section. MIS will ensure that wireless access points adhere to departmental policies and statewide information security standards.
- d. Wireless access points shall only be installed, managed, maintained, and configured by authorized MIS personnel or by an MIS approved vendor.
- e. Wireless access points shall only be active during approved time periods.

2. Device Usage

- a. For any wireless network designated exclusively for use by DPS employees, only DPS authorized devices shall be allowed to access the wireless network.
- b. Where available, guest wireless access (Internet Only) shall be used by guests of the department. Examples of guests include vendors, visitors, and other government employees. Guests are required to review wireless access entry screens and must agree to all terms and conditions before accessing the wireless network.
- c. If personal devices are used to access a DPS wireless network, employees will utilize the guest wireless network. All applicable DPS policies regarding the use of personal devices must be adhered to. These policies include, but are not limited to:
 - Network Security Use Policy
 - Internet Acceptable Use Policy
 - Email Acceptable Use Policy
 - Remote Access Policy
 - Laptop and Mobile Device Use Policy

Only moderate personal use of a DPS wireless network is allowed and **excessive personal use is prohibited.**

3. Monitoring/Management

- a. MIS monitors the department's network. If MIS discovers unauthorized or inappropriate wireless transmissions at a DPS facility, MIS will take all reasonable attempts to notify the appropriate user and/or manager. If the unauthorized transmission causes interference and/or compromises security, MIS may take action to immediately terminate the wireless signal.