Wireless Access Policy
USG Policy 6 (3.60) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to state the standards for wireless access to USG's network.

This policy covers anyone who accesses or utilizes the USG network via an 802.11 wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Mac Address*: short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

B. *SSID*: stands for Service Set Identifier. The name that uniquely identifies a wireless network.

C. *WEP***:** stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

D. *Wi-Fi:* short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

E. *Wireless Access Point:* a central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

F. *Wireless NIC*: a Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

G. *WPA*: stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

III. Physical Guidelines

A. Physical security of access points must be considered. Access points must not be placed in public or easily accessed areas unless physically secured. Unsecured access points must be placed in non-obvious locations (i.e., above ceiling tiles) so that they cannot be seen or physically accessed without difficulty.

IV. Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

A. Security Configuration

1. The Service Set Identifier (SSID) of the access point may or may not be broadcast. Broadcast SSIDs are easier for guests to locate and join and thus provide a service to the USG community. Non-broadcast SSIDs are used for networks to which guests are unlikely to need access, thus keeping their Wi-Fi network pick list cleaner. Not broadcasting an SSID is not a security feature and must not be treated as such.
2. Encryption must be used to secure non-public wireless communications. Stronger algorithms are preferred to weaker ones (i.e., WPA2 should be implemented rather than WEP). Encryption keys for shared-key implementations must be changed and redistributed semi-annually.
3. Administrative access to wireless access points must utilize strong passwords and follow the USG Password Policy 6 (3.40).
4. Logging features should be enabled on the USG Wi-Fi system.
5. Different SSIDs may be used to differentiate access to separate USG network security zones provided they are in compliance with USG's Network and Systems Security Policy 6 (3.30).

B. **Installation**

1. Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
2. Wireless networking must not be deployed in a manner that will circumvent USG's security controls.
3. Wireless devices must be installed only by USG's OIT department. Installation of wireless devices by non-OIT personnel which allow access to the USG network is expressly prohibited.
4. Channels used by wireless devices should be evaluated to ensure that they do not interfere with USG equipment or violate the Wi-Fi channel plan.

V. Accessing Confidential Data

A. Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data, such as, the USG Confidential Data Policy 6 (2.00).

VI. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VII. Revision History

Date	Description	Revised By
07/25/2018	Initial Policy Creation	Russell Schlosburg

VIII. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf