WIRELESS POLICY

Version number	Review date	Reviewed by	Approval date	Approved by	Summary of Changes	Next review date
1.0	Jul 2012	G. Price	Jul 2012	J. Ilag	Baseline	
2.0	Dec 2015	G. Price	Jan 2016	J. Ilag	No change	Jul 2017

A. Policy objective:

1. The purpose of this policy is to secure and protect information assets which are transmitted over airwaves. Access to wireless resources is a privilege and must be managed responsibly to maintain confidentiality, integrity, and availability. This policy specifies the conditions that wireless infrastructure devices must satisfy in order to connect to UNFPA's network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the MIS Branch are approved for connectivity to UNFPA's network. Current wireless standards can be found here: https://portal.myunfpa.org/web/mis/guidelines

B. Intended audience:

2. All staff, vendors, consultants, temps, guests, and other workers in UNFPA must adhere to this policy. This policy applies to all users of wireless infrastructure devices that connect to UNFPA's HQ or field networks that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

C. Policy statement:

a. Ownership:

3. UNFPA wireless infrastructure is owned by the organization. Technical approval for major configurations and design must be obtained from the MIS Technology Services Section prior to implementation.

b. Monitoring:

4. UNFPA reserves the right to monitor wireless use and provide identification of unauthorized use without notice. Consistent with generally accepted business practices, UNFPA collects data about its wireless infrastructure and technical staff monitors its use to ensure security is maintained. Should a security or other relevant incident arise, UNFPA may review wireless system logs to determine the event cause and take other appropriate action. If it is determined, for example, that the security incident arose, in whole or in part, due to user noncompliance with applicable regulations, rules, policies or procedures, this may result in forfeiture of the privilege to use technology resources as well as administrative, disciplinary or other legal action as applicable.

c. Security:

5. Wireless access points must be installed by UNFPA ICT staff or authorized contactors. Installation must be on a different firewall segment from internal network users. Whenever possible, wireless access points should be located towards the center of the office, thus limiting the ability to detect and access the network from outside the office. Wireless access points shall require user authentication at the access point before granting access. At a minimum, WPA2 wireless security must be enabled on wireless access points. Wireless passwords and data must be encrypted. No application should rely on IP address based security or reusable clear text passwords. Wireless access point passwords should be changed semi-annually.

6. Users must maintain the confidentiality of wireless passwords. It is important to be aware that public wireless is not secure, and information transmitted may be read by others.

d. Responsible Use:

7. UNFPA provides wireless access to users and guests to facilitate business communications and assist in performing daily work activities. The same provisions regarding the ethical use of UNFPA hardware and software pertain and are applicable to wireless users.

D. Related Policies

8. ICT Hardware Policy (http://www.unfpa.org/sites/default/files/admin-resource/MIS_Hardware%20Policy_0.pdf)
9. ICT Software Policy (http://www.unfpa.org/sites/default/files/admin-resource/MIS_Software%20Policy_0.pdf)
10. BYOD policy (https://www.myunfpa.org/web/ppm/documents/tags/mis)

E. Policy date:

11. The Wireless Policy (originally approved and issued on 18 July 2012 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

F. Policy owner:

12. The MIS Infrastructure/Security Specialist is responsible for ensuring wireless functionality.

G. Change authority:

13. The Technology Services Section Chief and Infrastructure/Security Specialist have the authority to change the policy. The MIS Chief and Business Services Section Chief can give exception waivers to it.