Network Security

Firewalls and Traffic Control

1 An appropriate network segmentation must be implemented for network infrastructure in accordance with risk assessment.
2 Traffic between different network segments must pass via network firewall(s).
3 Additional security mechanisms can be implemented for traffic between different network segments in accordance with risk assessment.
4 Systems must be hosted in an appropriate network segment in accordance with risk assessment.
5 Internal systems and services must not be exposed directly to untrusted networks.
6 Internal systems and services must not access untrusted networks directly.
7 Access to public internet by internal systems, users, and devices must go through an approved standard web proxy. Internal systems, users, and devices must not access the Internet directly.

Guest Wi-Fi and Wired network security control requirements

Purpose

8 The purpose of the Guest Wi-Fi and Wired security control requirements document is to provide a WHO security standard for creation and operation of Guest Wi-Fi and Wired Networks.
9 Guest Wi-Fi and Wired networks (public networks for WHO visitors) are intended to provide quick and easy Internet access for visitors.
10 WHO visitors must exclusively have access to Guest Wi-Fi or Guest wired networks, and never to networks intended for the WHO workforce.
11 WHO is not responsible for the privacy of data exchanged via Guest networks. Visitors are expected to exercise due diligence (use of secure protocols, VPN, MFA, etc.) when using WHO Guest networks.
12 WHO may monitor traffic from devices connected to guest networks and disconnect devices consuming too much bandwidth or performing malicious activities.

13 This document shall be read in conjunction with the rest of the WHO Global Cybersecurity Policy.

Scope

14 Security control requirements are applicable to all WHO employees, contractors, and visitors ("users") when Guest Wi-Fi and/or Wired networks are used in WHO offices.

Security Controls

15 The following mandatory controls must be applied to both Guest Wi-Fi and Wired networks:

16 Guest networks must use a separate physical or virtual (VLAN) network.

a. Guest networks must be connected to a dedicated firewall interface.
b. Appropriate global network security controls (exp. DNS Filtering) must be enabled for
c. Traffic originating from a guest network.
d. Guest networks must not provide direct access to internal WHO services.
e. Firewall policy for Guest network must be explicit and must not allow any protocols and services not listed in Annex 1.
f. Annex 1 can be updated with the approval of the Cybersecurity team.

17 The following mandatory controls must be applied to Guest Wi-Fi network:

a. Traffic between devices connected to the same Guest Wi-Fi network must not be permitted.

18 The following optional controls may be applied to Guest Wi-Fi network:

a. Guest Wi-Fi should not require authentication, as so to encourage its use over internal Wi-Fi.
b. In case access to the Guest Wi-Fi network needs to be limited, Guest Wi-Fi may be secured with a password and WPA2 enabled.
c. If a Guest Wi-Fi password is enforced, the password must be changed periodically. The recommended maximum password duration is 3 months. Passwords cannot be reused.

Compliance

19 Refer to the compliance section at Global Cybersecurity Policy.