Wi-Fi Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | Approved by: |
| 1.0 | 12/12/2021 | D Henderson | Initial document |  |
| 1.1 | 30/09/2022 | D Henderson | Added inline version history and document owner |  |

Document Owner **IT**

# Introduction

Wi-Fi is a highly adopted technology. Its use has been identified to offer benefits to MLPC.   
  
This policy is to ensure that the development and use of wireless networking and its use is controlled and managed in a centralised way to provide the best level of service and performance whilst maintaining adequate levels of security. Unlike other network devices Wi-Fi access is accessible to all, however like all other aspects of networking in it not acceptable practice to allow the installation or operation of wireless devices on Microlink premise or attached to Microlink network without a clear and approved policy outlining the roles and responsibilities of all parties.  
  
The policy is maintained by IT department and approved by Senior Management.

# Policy Objectives

* 1. The policy sets out to outline procedures and operation criteria to effectively manage WiFi within the organisation all wireless deployments must be carefully planned deployed and managed in a carful and controlled manner
     1. **Performance:**  WiFi operates using different frequencies, these frequencies are then split up into bands. To maintain reliable performance devices, need to be configured in such a way that the WiFi bands do not overlap. These bands need to be assigned by IT to ensure performance is not impacted.
     2. **Security concerns** 
        1. **Perimeter less networks** wireless networks offer connectivity to anyone within range of a Wi-Fi access point. Physical boundaries, including site parameters, are no longer a relevant location to prevent access to the network. Various controls need to be implemented depending on risk associated with it.
        2. **Unapproved devices** with little or no security, if connected to the corporate network would pose a threat or create an “open door” to our network. Various controls are required to ensure Microlink’s system remain safe whilst providing valuable services to staff and visitors.

# Policy

## Scope

This Wi-Fi 802.11 policy applies to all areas of wireless connectivity to the Microlink network infrastructure. And applies to all wireless devices that operate on Microlink network at all Microlink premises or remote locations that connect back to the Microlink network.

Microlink Internal IT are responsible for all Microlink network infrastructure. This includes all wireless network infrastructure by extension. Microlink Internal IT have the sole responsibility for the design, implementations, and maintenance of all Microlink LANs.

## Restrictions

* + 1. All access points must comply with national regulations regarding to wireless devices.
    2. Installation of access points onto any Microlink network must be authorised and conduct by Internal IT, this includes on premise or where a network connection is made remotely.
    3. Unauthorized access point will be removed from the network without warning.
    4. Only Meraki based Access point that are attributed to Microlink subscription are to be used.
    5. Proactive monitoring of wireless networks will be regularly carried out.
    6. All requests for new WiFi requirements including but not limited to New access point, New network SSIDs, must be directed through Internal IT via IT Tickets.
    7. Internal IT acts as a central management body in the regulating, installation and maintenance of all network technologies including WiFi.
    8. Authentication to corporate networks must use WPA2-Enterprise 802.11X – certificate-based authentication Authorized by RADIUS server.  
       1. Certificates are to only be issued to Company workstations and laptops.
    9. Internal IT have the right to employ active counter measures to defend against rogue Access points being attached to the network.
    10. Microlink reserve the right to monitor and record wireless and internet access to ensure policy compliance in accordance with privacy, anti-hacking, and data protection legislation.
    11. Microlink reserve the right to limit bandwidth of wireless devices, as necessary, to ensure network reliability and fair usage of network resources.

# Network Acceptable use

To maintain security and reduce risk to Microlink systems several isolated networks have be created for different uses. The following outline each network and is acceptable use. Any use case not explicitly stated below is prohibited unless authorised by Internal IT.

* 1. **All networks** 
     1. All activities must comply with national legislation including but not limited to
* Computer misuse act 1990.
* The Data Protection Act 2018.
  + 1. Misuse must be reported to IT immediately.
    2. Users must ensure that all practical steps necessary to make sure that equipment connected to the service is secure (this includes up-to-date anti-virus software and system updates)
    3. Users will respect system security and will not disclose any passwords or security information provided to access wireless services.
  1. **Microlink Main** 
     1. Only Microlink Laptops and wireless workstations are authorised to run on this network.
     2. Network is for the purposes of conducting Microlink business only.
     3. Secured using Certificate based WEP-Enterprise authentication.
  2. **Microlink Guest**
     1. This network is for personal devices of staff or visitors.
     2. Network is for the purposes of personal use
     3. Should only be accessed from public/recreational areas of the business.
     4. Network is isolated and only supplies internet access.
     5. Secured using a pre-shared key.
  3. **Repairs/Production Wi-Fi**
     1. This network is for machines that require loading or repairs only.
     2. Personal devices are prohibited from this network.
     3. Network is isolated and supplies access to production/repairs network and the internet.
     4. Secured using a pre-shared key
  4. **DemoNet**
     1. This network is for Demonstrating equipment.
     2. This network is isolated and supplies access to the demo network.
     3. Secured using a pre-shared key.
  5. **Datalinx**
     1. This network is for warehouse PDAs only
     2. This network is isolated and supplies access to sage API.
     3. Secured using a pre-shared key

# Roles and responsibilities

## Internal IT responsibilities.

* + 1. All LAN, wireless or wired are the responsibility of Internal IT. Any network devices or access points connected to the network becomes the responsibility of Internal IT. Either to remove it or support it.

## User responsibilities

The following restriction apply to all users of the organisation’s networks.

* + 1. Personal devices (Devices not owned by Microlink) are only allowed on the “Microlink Guest” network.
    2. Acceptable use policy must be accepted and followed before use.
    3. Corporate networks, networks where corporate resources are available, may only to by a domain-controlled workstation or laptop that have been issued a network access certificate.

# Policy Violations

Any violation of this policy should be brought to the attention of the Head of IT and the Information Security Manager, who will work with the relevant department heads or appropriate individuals to rectify the problem.