Device Hardening Policy

All Devices connecting to Microlink data systems must be hardened according to the following guidelines where appropriate.

# 1 Internal device.

* 1. Restrict network access to the minimum number of subnets practical for the device to function for its users.
  2. Firewalls must be installed and only required ports opened.
  3. Management/configuration access must be restricted via VLAN or only to restricted machines
  4. Use secure protocols when transmitting network device configuration files.
  5. Shut down unused physical interfaces on network devices
  6. Only use secure protocol standards (SSHv2; IKEv2/IPsec; TLS v1.0+) when performing remote management of network devices.
  7. Default usernames/passwords should be changed and logged in the password vault.
  8. Ensure that all network infrastructure devices create an audit event when configuration changes are applied, when operating system firmware is upgraded, and when the device is rebooted.
  9. Web Accessible Devices must be placed within the DMZ where possible.

# External devices

* 1. External devices connecting to Microlink Data Systems must be approved by IT and verified as secure as per the mobile device policies.
  2. Weak Ciphers, Weak Cipher suites, Weak Key Exchange protocols and Weak hashing algorithms should be removed.
  3. Only secure protocol standards should be used. (TLS 1.2 etc)

# All devices

* 1. All devices must be kept on latest, approved, and tested firmware/software versions.
  2. That have firewall should be kept enabled and only required ports opened.
  3. Must be placed on a suitable vLAN based on its risk and use.
  4. Unrequired services should be uninstalled or disabled.