# Wireless Access Policy

## Overview

Wireless technology provides a convenient mechanism for accessing user resources. These technologies have become ubiquitous in the workplace environment. The advent of wireless technologies adds increased functionality but also adds security risks and concerns that must be managed and mitigated.

## Purpose

This policy provides a set of procedures and standards for implementing wireless technologies within the [LEP] network environment. It provides network administrators who deploy and manage wireless technologies with a baseline set of requirements that document connectivity, security, and device oversight.

## Scope

This policy applies to all [LEP] staff who engineer, install, or support wireless networks.

## **Policy**

### INTRODUCTION

By using wireless devices within the [LEP] network for business purposes, all staff are subject to policies managing their use. All wireless devices including personal smartphones, tablets, or other devices are subject to the guidelines and procedures set forth in this policy.

### CONNECTIVITY CONSIDERATIONS

Wireless networks are comparatively limited in speed, bandwidth, and coverage to wired networks. Where possible, the use of a wired connection is preferred because it is faster and does not compete with other wireless devices for bandwidth. However, use of wireless devices is increasing as it provides a convenient mechanism for accessing resources. Along with this convenience is a need for managed security as the devices are natively less secure than a hardwired device. The following procedures and practices shall be implemented to reduce risks related to wireless networks:

* Wireless networks shall be segmented between external guest and internal networks. Non-[LEP] devices shall not be connected to the [LEP]’s internal network
* Users inside the [LEP] firewall shall not connect to the internal network if they are using a bridged wireless connection to connect to an external network
* Wireless access points or routing devices with wireless capability are not allowed unless approved by the [Insert Appropriate Role or Department]
* Logical and physical user access to wireless network devices shall be restricted to authorized personnel and devices excepting for access to a guest network
* Perimeter firewalls shall be implemented and configured by support staff to restrict unauthorized access and traffic metering
* All vendor default settings for wireless devices (e.g. passwords, wireless encryption keys, SNMP community strings) shall be changed prior to installing wireless equipment in a production environment
* Wireless security protocols shall be used that are of the highest encryption possible
* Strong passwords shall be employed for all wireless SSID and changed on a periodic basis either through the protocol or across the enterprise
* Ad-hoc [LEP] wireless device audits shall be conducted on at least a quarterly basis to determine if any rogue devices exist on the [LEP] network
* Findings shall be presented immediately to the [Insert Appropriate Role] and all rogue devices removed from the network

### SECURITY

Wireless (Wi-Fi) transmissions used to access [LEP] networks and devices shall be encrypted. If sent across a public or open network, both the authentication data (e.g. a user ID and password) and the data itself shall be encrypted with strong encryption. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission security protocols along with approved encryption techniques are utilized.

The [Insert Appropriate Role] or their designee shall ensure:

* Sensitive information is encrypted using the strongest and most cost effective encryption available
* Wireless networks transmitting sensitive information or connected to sensitive information environments, use industry best practices to implement strong encryption for authentication and transmission
* Processes test for the presence of rogue wireless access points and detect and identify all authorized and unauthorized wireless access points
* Procedures maintain an inventory of authorized wireless access points including a documented business justification
* Response procedures exist and are implemented in the event unauthorized wireless access points are detected
* Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

* Spot user checks for compliance with this policy
* Archival documentation of quarterly checks and any remediation required
* Anecdotal communication evidence of policy implementation via email, logs, or other documentation

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 8/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |