Wi-Fi Deployment and Security

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series
An exclusive publication of Sandbox Technologies, Inc.
3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Table of Contents

Wi-Fi Deployment & Security....3
When it goes wrong....4
- The Evil Twin in the Lot....4
- The Guest Who Reaches the Server....4
- The Access Point Nobody Approved....4
- The Network That Just Feels Slow....4
- The common thread....4

What to Ask Your IT Manager or Provider....5
- Requirements & Equipment Analysis....5
- Site Survey & Placement....5
- Tuning & Optimization....5
- Enterprise-Class, Controller-Based Solution....6
- Current-Generation Encryption....6
- Segmentation from the Corporate Network....6
- Guest and Personal-Device Network....7
- Rogue and Unauthorized Access Points....7
- No Automatic Connections....7
- Default Passwords and Rotation....8
- Wireless Flood Protection....8

Terminology....8
- WPA3, WPA3-Enterprise, WPA3-Personal....8
- WPA2, WPA2-Enterprise, WPA2-PSK....8
- Wi-Fi 6, 6E, and 7, and the 6 GHz band....8
- Controller-based network....9
- Site survey....9
- Evil twin....9
- The Site Survey....9
- Why Placement Is Not Obvious....9
- Frequencies and Tuning....9
- Segmentation and Access....9

© 2026 Sandbox Technologies, Inc.

Wi-Fi Deployment & Security

The one part of your network a stranger can reach from the parking lot

Consumer wireless gear is easy to buy and easy to plug in, and that ease is exactly what leads businesses to underestimate it. A wireless signal does not stop at the walls, and the same network can quietly underperform for years, or quietly expose the company for just as long. Both outcomes are decided at deployment, not by the box the equipment came in. The situations below are more common than most organizations realize.

© 2026 Sandbox Technologies, Inc.

When it goes wrong

Not every network needs enterprise hardware in every corner, and a modest setup is often an acceptable, deliberate choice. The point is not to alarm. It is to make sure the exposures below are ones the organization understands and accepts, rather than ones it never saw.

The Evil Twin in the Lot

A laptop is set to reconnect to known networks on its own. Someone nearby runs a device that broadcasts the same network name at higher power. The laptop trusts the stronger signal and connects, and the operator simply accepts whatever it sends.

The Guest Who Reaches the Server

A visitor's laptop, or an employee's personal phone, joins a wireless network that is bridged to the main company network. The device is unmanaged, and no one can vouch for what it is carrying.

The Access Point Nobody Approved

An employee wants better signal in a back office and plugs a consumer access point into a live wall jack. It arrives with good intentions, no encryption discipline, and no oversight.

The Network That Just Feels Slow

No site survey was done. Access points were placed by guesswork and left on default channels that compete with the neighbors. Calls drop, transfers crawl, and everyone assumes that is simply how Wi-Fi behaves.

The common thread

None of these is a story about a faulty product. Each traces back to decisions made once, at deployment, about how the network was surveyed, placed, segmented, encrypted, and governed, and then rarely revisited.

A wireless network reaches past your walls whether you planned for it or not. Whether that reach becomes an exposure is decided by how the network is deployed and secured, not by the equipment on the box. That is the entire point of this issue.

© 2026 Sandbox Technologies, Inc.

What to Ask Your IT Manager or Provider

and how to know if the answers are good ones

You do not need to administer a wireless network to oversee one. You need to know what to ask. A fuller primer on encryption, site surveys, and the terms your IT team will use is provided at the end, for those who want the detail. First, the part that matters: run the checklist below with your IT professional. If any item is not marked green, it may warrant a closer look.

Requirements & Equipment Analysis

Was a professional requirements analysis performed before any wireless equipment was selected? The right solution depends on details that are easy to skip: how many devices each access point must support at once, antenna and power requirements, signal-tuning capability, how the equipment interoperates with the firewall and core network, and whether a single set of credentials must work across multiple sites. Equipment chosen without this analysis often has to be worked around later.

Compliant	NOTES:
Needs Attention	
N/A	

Site Survey & Placement

Was a professional site survey conducted before structured cabling was installed and access points were mounted? Placement decides performance, and closer is not always better. Building materials such as plaster over metal lath, concrete, mirrored glass, and steel framing all block or distort signal, and access points sited too near one another can interfere. A survey establishes where coverage will actually hold before anything is cabled in.

Compliant	NOTES:
Needs Attention	
N/A	

Tuning & Optimization

Has the network been tuned for its environment rather than left on factory defaults? Professional equipment can be adjusted to avoid interference from neighboring networks sharing the same channels, and the different frequency bands trade range against the ability to pass through walls. A network that was never tuned often underperforms in ways that look like a hardware fault but are not.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Enterprise-Class, Controller-Based Solution

Is the network built on enterprise-grade, controller-based equipment rather than a collection of standalone consumer units? A controller, on premises or in the Cloud, provides centralized control, more granular security and tuning, better visibility into anomalies, and a simple way to push critical updates. It also helps catch a single misconfigured access point before it becomes an exposure.

Compliant	NOTES:
Needs Attention	
N/A	

Current-Generation Encryption

Is the wireless network using the current generation of encryption its hardware supports? WPA3, in its WPA3-Enterprise or WPA3-Personal form, is now the current standard and is recommended wherever equipment supports it; on the 6 GHz band used by Wi-Fi 6E and Wi-Fi 7, WPA3 is required. WPA2-Enterprise with AES remains an acceptable minimum on older 2.4 and 5 GHz hardware, but WPA2 is no longer the latest generation. WPA2-Personal (often labeled WPA2-PSK) will typically pass a casual audit yet remains more exposed to password attacks, and the older WEP and WPA protocols should be treated as obsolete. No wireless network is ever entirely secure, so it is recommended that organizations run the most current encryption their equipment supports.

Compliant	NOTES:
Needs Attention	
N/A	

Segmentation from the Corporate Network

Is wireless access segmented from the corporate network (the LAN) by a firewall? Wireless traffic can be exposed to interception, man-in-the-middle attempts, and denial-of-service traffic, so it is generally recommended that wireless devices reach internal resources only through a VPN client or an approved remote-access solution, rather than sitting directly on the LAN.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Guest and Personal-Device Network

Is there a separate, Internet-only network for guests and for employee-owned devices that are not authorized on the company network? Personal phones and laptops cannot be assumed to be patched, managed, or free of malware. Keeping them on their own segment removes an easy pivot point onto company-owned equipment.

Compliant	NOTES:
Needs Attention	
N/A	

Rogue and Unauthorized Access Points

Are there policies and technical controls to prevent unauthorized access points from being added to the network? Well-meaning employees have been known to plug consumer access points into live jacks for their own convenience, and someone with physical access to an open port could do the same with intent. Either creates exposure the organization did not choose. Controller-based systems can also detect rogue access points broadcasting nearby.

Compliant	NOTES:
Needs Attention	
N/A	

No Automatic Connections

Are company-owned devices configured not to connect or reconnect to wireless networks automatically? Automatic reconnection is convenient, but it is exactly what an evil-twin attack relies on: a rogue access point broadcasting the company network name at higher power, which a device then trusts as the closer, legitimate network. Disabling it is inconvenient and, for sensitive environments, worth it.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Default Passwords and Rotation

Have all default passwords been removed from access points, controllers, and switches, and are administrative and user passwords changed on a defined schedule? Default credentials left in place are among the simplest and most damaging oversights at deployment. Wireless passwords should also meet the organization's standards for length and complexity.

Compliant	NOTES:
Needs Attention	
N/A	

Wireless Flood Protection

Is wireless flood protection enabled? Though less common, flood attacks disrupt service by rapidly and repeatedly attempting to authenticate to access points, often using spoofed device identifiers so each attempt appears to come from a different, legitimate device. Enterprise equipment can be configured to absorb and blunt this.

Compliant	NOTES:
Needs Attention	
N/A	

Terminology

WPA3, WPA3-Enterprise, WPA3-Personal

WPA3 is the current generation of Wi-Fi encryption, the successor to WPA2. WPA3-Enterprise authenticates each user against a central directory (using 802.1X and a RADIUS server) and suits organizations; it also offers an optional 192-bit high-security mode. WPA3-Personal uses a single shared passphrase but strengthens it with a method called SAE (Simultaneous Authentication of Equals), which resists the offline password-guessing that affects WPA2-Personal.

WPA2, WPA2-Enterprise, WPA2-PSK

WPA2 is the prior generation and still widely deployed. WPA2-Enterprise with AES remains an acceptable minimum on older hardware. WPA2-PSK (a shared password) will often pass a casual audit but is more exposed to eavesdropping. The older WEP and WPA protocols are obsolete.

Wi-Fi 6, 6E, and 7, and the 6 GHz band

These are recent generations of Wi-Fi. Wi-Fi 6E and Wi-Fi 7 can use a newer 6 GHz band, on which WPA3 is required and WPA2 is not permitted. Hardware supporting these standards is increasingly common in new deployments.

© 2026 Sandbox Technologies, Inc.

Controller-based network

A design in which access points are managed centrally by a controller (on site or in the Cloud) rather than each being configured on its own. It is the basis of most professional deployments.

Site survey

A structured assessment of a space that maps where signal will reach and where it will be blocked, used to decide how many access points are needed and where to place them.

Evil twin

A rogue access point that impersonates a legitimate network by broadcasting the same name, usually at higher power, to lure devices into connecting to it.

The Site Survey

For anything beyond a small space, the recommended practice is to obtain professional floor plans (CAD is ideal, PDF is workable), import them into site-survey software, tag the materials and features that impede signal, and model each device's broadcast strength to produce a formal report. That report, not guesswork, should drive where access points are placed.

Why Placement Is Not Obvious

Closer is not always better. Access points positioned too near one another, or too near the devices they serve, can degrade performance. Wireless is also two-way: strong signal from the access point does not help if the device cannot broadcast back with comparable strength. Where mesh equipment must be used in place of hardwired access points, expect some performance loss each time one access point is chained to another to extend range. Hardwired access points remain the preferred approach.

Frequencies and Tuning

Higher frequencies carry more data and travel faster but pass through walls less well; lower frequencies reach farther and penetrate better but carry less. Tuning channels and power to the building, and away from competing neighbor networks, is what turns capable hardware into a network that performs.

Segmentation and Access

Because wireless is exposed to interception, man-in-the-middle attempts, and denial-of-service traffic, it is generally kept separate from the corporate LAN, with access to internal resources brokered through a VPN or an approved remote-access solution. Guest and personal devices belong on their own Internet-only segment.

© 2026 Sandbox Technologies, Inc.

© 2026 Sandbox Technologies, Inc.

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2026 Sandbox Technologies, Inc.