

Best Practice Checklist Series - Issue 7

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 reconnects to a familiar network name without properly authenticating it. An impostor lures it into connecting. A copied name or stronger signal alone does not defeat correctly configured authentication.

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 wireless encryption and authentication securely configured? Prefer WPA3 where compatible: Enterprise provides individual authentication, while Personal uses SAE and a passphrase. In 6 GHz, use WPA3 or Enhanced Open (OWE), not WPA2. OWE encrypts the radio link without authenticating the network or user; it is not equivalent to an authenticated corporate network. For legacy 2.4 or 5 GHz devices, assess WPA2 with AES and strong authentication while planning upgrades. Avoid WEP, original WPA and TKIP. Manage shared passwords carefully and check actual audit requirements.

Compliant	NOTES:
Needs Attention	
N/A	

Segmentation from the Corporate Network

Are wireless clients given only the access appropriate to their identity, device management and business need? Keep guest and unmanaged devices separate from sensitive resources, with controls enforced and tested. Managed corporate Wi-Fi can support authorized LAN access; a VPN is one possible design, not a requirement for every wireless client.

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

Do company-owned devices use approved wireless profiles and reject untrusted networks or certificate prompts? Limit automatic connection to approved networks, and validate the authentication server for enterprise Wi-Fi. A copied network name and stronger signal do not bypass proper authentication. Review saved profiles and disable unnecessary auto-join.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Default Passwords and Rotation

Have default credentials been replaced with long, unique administrative credentials? Do not require routine password changes without a risk or policy basis; change credentials after suspected exposure or relevant access changes. Manage shared Wi-Fi passwords when users leave, and prefer individual enterprise authentication where appropriate.

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 with AES can support legacy 2.4 and 5 GHz devices when securely configured. Enterprise authentication gives individual identities; shared-password security depends on password strength and distribution. WEP, original WPA and TKIP are obsolete. Check actual audit requirements.

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

Wi-Fi 6E and Wi-Fi 7 can use 6 GHz where permitted. This band supports WPA3 or Enhanced Open (OWE), with protected management frames, but not WPA2. OWE encrypts the radio link without authenticating the network or user.

© 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-frequency bands often offer wider channels and more capacity, but do not make radio waves travel faster. Throughput also depends on channel width, signal quality, interference, spatial streams and device capabilities. Building materials and deployment conditions affect coverage; tune channels and power using survey measurements.

Segmentation and Access

Segment clients by trust, device management and business need on both wired and wireless networks. Enforce and test the allowed paths. Guest and unauthorized personal devices generally belong on an isolated internet-only segment. Managed corporate wireless devices may receive authorized internal access; a VPN is one possible access design.

© 2026 Sandbox Technologies, Inc.

Review your findings

Discuss items needing attention with your IT professional and assign next steps.

© 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.