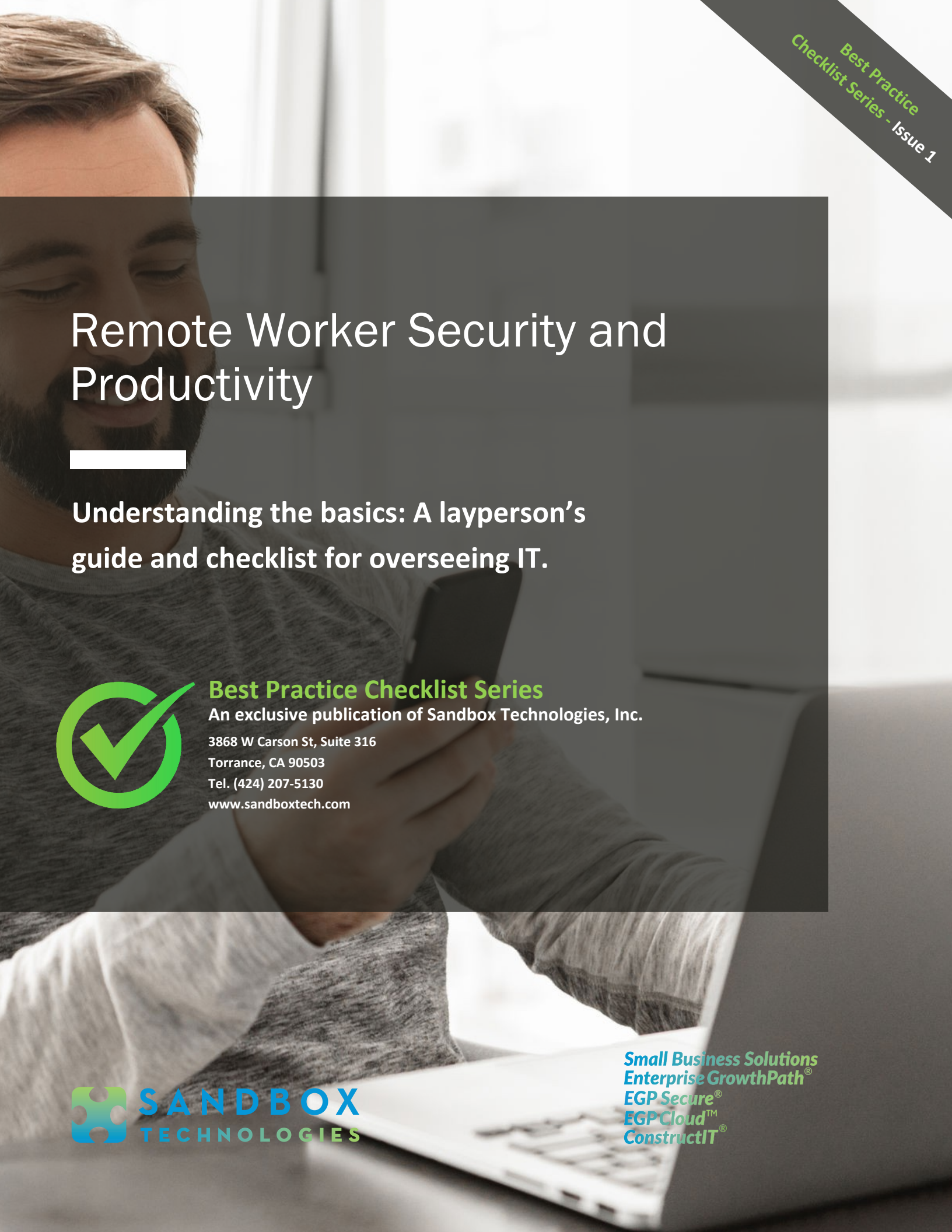


Best Practice Checklist Series - Issue 1

Remote Worker Security and Productivity

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

Remote Worker Security & Productivity 3
Where remote work quietly goes wrong 4
- The home network as a doorway 4
- The device the company cannot reclaim 4
- A stolen password and a weak second factor 4
- Protection that no one is watching 4
- The common thread 4

What to Ask Your IT Manager or Provider 5
- Target Computers 5
- Remote Computers 5
- Access Method 6
- Multi-Factor Authentication 6
- Connection Method at the Remote Location 6
- Remote Location Security 7
- Endpoint Protection 7
- Restricted VPN Scope 7
- Internet Connectivity at the Remote Location 8
- Segmentation of Devices 8

Overseeing productivity without overreaching 8
- Key Performance Indicators 9
- Proportionate Activity Visibility 9

Terminology 9
- Hosted Desktop (formerly Terminal Server) 9
- VPN and Zero Trust (ZTNA) 10
- Multi-Factor and Phishing-Resistant Authentication 10
- Endpoint Protection and EDR 10
- Network Segmentation 10
- Company-Owned Devices vs. BYOD 10
- Wi-Fi vs. Wired 10
- A Company-Managed Internet Circuit 11
- Firewall Trade-offs at Home 11

© 2026 Sandbox Technologies, Inc.

Remote Worker Security & Productivity

Your security perimeter now runs through networks you do not own

Remote and hybrid work is no longer a temporary arrangement. It is a permanent part of how most organizations operate, and it moved two things outside the walls of the office at once: the systems that must be secured, and the people who must be overseen. The security question is that a home network the company does not control is now part of its attack surface. The productivity question is quieter, that a manager loses the incidental visibility a shared office provides. Both are manageable, and both are far easier to get right on purpose than to fix after something goes wrong.

© 2026 Sandbox Technologies, Inc.

Where remote work quietly goes wrong

Not every remote setup needs every safeguard, and some exposure is a reasonable trade for speed and cost. The point is not to alarm. It is to make sure each trade was chosen deliberately, because the situations below are more common than most organizations expect.

The home network as a doorway

A work laptop shares a flat home network with a smart TV, a game console, and a router still using its factory password. One of those devices is compromised, and because nothing separates them, the attacker moves sideways onto the laptop, and from there toward the company network.

The device the company cannot reclaim

Work is done on an employee's personal computer. When that person leaves, or is suspected of wrongdoing, the company has no clear right to inspect, wipe, or recover the machine, and the company data on it goes too.

A stolen password and a weak second factor

A reused password is phished. If no multi-factor authentication stands behind it, or if the second factor is a simple approve prompt the user taps without thinking, the attacker signs in from anywhere as a trusted employee.

Protection that no one is watching

Security software is installed on each remote machine, but no one confirms it is switched on, current, and actually running. An infection spreads on a device everyone assumed was covered.

The common thread

None of these is a story about expensive tools or sophisticated attackers. In each case the exposure traces back to a single control that was left optional, unmanaged, or invisible, on equipment and networks the company does not own.

Every one of these outcomes is avoidable, and rarely by spending more. They come down to a short list of choices about who owns the device, how it connects, and who is actually watching it. That is what the checklist below is for.

© 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 remote-access environment to oversee one. You need to know what to ask. A short primer on the terms 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.

Target Computers

Is remote work delivered through properly secured company workstations or a suitably configured hosted desktop, rather than uncontrolled personal machines? A hosted desktop (Remote Desktop Services, Azure Virtual Desktop, or Windows 365) keeps the data in a managed environment instead of on the endpoint.

Compliant	NOTES:
Needs Attention	
N/A	

Remote Computers

Are the devices used for company work owned and managed by the organization rather than employee owned? Company ownership preserves the ability to harden, encrypt, monitor, and reclaim the device.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Access Method

Has the organization standardized on a secure remote-access platform suited to its needs? An encrypted VPN, or a Zero Trust Network Access (ZTNA) solution, paired with restricted remote desktop access, is appropriate in many situations. The method chosen decides how much of the network a compromised endpoint can reach.

Compliant	NOTES:
Needs Attention	
N/A	

Multi-Factor Authentication

Is access to every company resource protected by multi-factor authentication, ideally a phishing-resistant method such as a hardware security key or passkey, or number-matching rather than a simple approve or deny push? MFA blocks most stolen-password attacks, but attackers increasingly target weaker factors and push fatigue.

Compliant	NOTES:
Needs Attention	
N/A	

Connection Method at the Remote Location

Where practical, are remote devices connected by wired Ethernet rather than Wi-Fi, and where Wi-Fi is unavoidable, is it secured to WPA3 where available and WPA2 at a minimum? Residential Wi-Fi is frequently the weakest link in a remote setup.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Remote Location Security

Is the remote device protected by a company-owned and managed firewall appliance, or at a minimum a properly configured software firewall? Many home networks have little or no perimeter protection at all.

Compliant	NOTES:
Needs Attention	
N/A	

Endpoint Protection

Is the device protected by a centrally managed endpoint protection solution, ideally one with detection-and-response (EDR) capability, that is actively monitored and kept current? Standalone antivirus with no central visibility cannot be confirmed to be working.

Compliant	NOTES:
Needs Attention	
N/A	

Restricted VPN Scope

If a hardware VPN is in use, is its traffic restricted to a designated work device at the remote location? An unrestricted tunnel effectively extends the corporate network to every device in the home.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Internet Connectivity at the Remote Location

Where feasible, is Internet connectivity at the remote location provided and managed by the organization? A dedicated circuit separates business traffic from the household and simplifies both security and support.

Compliant	NOTES:
Needs Attention	
N/A	

Segmentation of Devices

Are business devices segmented from all other Internet-enabled devices on the remote network (personal computers, phones, streaming and other appliances, smart TVs, and similar)? Segmentation keeps a compromise on one device from spreading to the work device.

Compliant	NOTES:
Needs Attention	
N/A	

Note: In some jurisdictions, employers may be required to provide or reimburse remote employees for the equipment and services needed to perform their work. Sandbox Technologies does not provide legal advice; organizations should consult their own counsel regarding obligations under applicable law before implementing these measures.

Overseeing productivity without overreaching

measuring outcomes, and coaching before problems harden

The harder half of remote work is often not technical. In a shared office, a developing problem tends to get noticed in passing. At a distance, the same problem may surface only when a deadline slips. The goal here is not to watch people. It is to notice a genuine issue early enough to coach rather than discipline, and to do so with the least intrusion that answers the question.

Clear performance indicators are the most effective and the fairest measure, because they judge outcomes rather than motion. Some are difficult to capture until a problem is already visible, and defining them is largely a management and human-resources exercise, though software can assist. When a specific concern does arise, a proportionate review of activity can help separate a real problem from an innocent explanation. Aggressive tools that capture every keystroke and continuous video exist, but they are costly to store and, for most organizations, more than the question requires. Lighter solutions that log basic activity and occasional screenshots are usually enough to surface a problem in time to address it.

© 2026 Sandbox Technologies, Inc.

Sandbox produced the example below to illustrate the point. It is an activity log for a fictional user, Bob Smith, whose supervisor would normally have no reason to request one. Lately, though, Bob has missed several deadlines. Read one way, the time on sports sites looks like distraction. Read another, it could be preparation for a meeting with a sports-minded client. An activity log is a tool for fairness as much as accountability, and it is only ever the starting point for a conversation, not the end of one.

Two questions are worth confirming for productivity, in the same spirit as the security checklist above.

Key Performance Indicators

Has the organization defined clear performance indicators for each role, and does it review and act on them routinely through supervisory staff? Outcome-based measures identify problems earlier, and more fairly, than watching activity.

Compliant	NOTES:
Needs Attention	
N/A	

Proportionate Activity Visibility

Where warranted, does the organization have a measured way to review user activity to identify and address problems, using the least intrusive level of monitoring that answers the question? Light-touch activity logs can surface an issue for coaching before it becomes a pattern.

Compliant	NOTES:
Needs Attention	
N/A	

Terminology

Hosted Desktop (formerly Terminal Server)

A hosted desktop delivers each user a virtual Windows desktop that runs on a central server rather than on the device in front of them. Microsoft's older name for this was Terminal Server; current forms include Remote Desktop Services, Azure Virtual Desktop, and Windows 365 Cloud PC. The data stays in a managed environment, which simplifies security and control and can let older hardware be re-purposed. The trade is that the host becomes a point of concentration that must itself be protected and kept available.

© 2026 Sandbox Technologies, Inc.

VPN and Zero Trust (ZTNA)

A VPN creates an encrypted tunnel between the remote device and the company network. It remains a sound tool, but a traditional VPN often grants broad access to the network once connected. Zero Trust Network Access (ZTNA) is a newer approach that grants access to specific applications rather than the whole network and re-checks trust continuously. Which one fits depends on the environment, and both are worth discussing with your IT professional.

Multi-Factor and Phishing-Resistant Authentication

Multi-factor authentication asks for something you know (a password) and something you have (a code or a device), so a stolen password alone is not enough. Not all factors are equal. Codes sent by text and simple approve or deny push prompts can be intercepted or worn down by repeated prompts, an attack sometimes called push fatigue. Phishing-resistant methods, such as hardware security keys and passkeys, or number-matching prompts, are markedly stronger and are now the recommended direction.

Endpoint Protection and EDR

Traditional antivirus matches known threats. Modern endpoint protection, often called EDR (Endpoint Detection and Response), also watches for suspicious behavior and can respond automatically. Managed centrally, it gives the organization the visibility that a standalone product on a remote machine cannot.

Network Segmentation

Segmentation keeps business devices on a separate logical network from personal computers, phones, and smart-home devices, so that a compromise on one cannot easily spread to the other.

Company-Owned Devices vs. BYOD

Company-owned, managed devices can be hardened, patched, encrypted, monitored, and reclaimed. Personal devices under a Bring Your Own Device (BYOD) agreement are difficult to secure to the same standard, may raise legitimate privacy concerns, and can leave the company without clear standing to inspect or recover a device on departure or when wrongdoing is suspected. Company ownership is generally preferable.

Wi-Fi vs. Wired

Home Wi-Fi is frequently the weakest link: default or shared passwords, dated equipment, and no separation between the work device and everything else on the network. Where Wi-Fi cannot be avoided, it should use WPA3 where available and WPA2 at a minimum, and business use should be limited to Internet access with no reach to other local devices. Where an Internet-of-Things device

© 2026 Sandbox Technologies, Inc.

such as a smart TV or streaming appliance must share the space, a separate network should be configured for it.

A Company-Managed Internet Circuit

A separate, company-provided Internet circuit at the remote location separates business traffic from the household, allows a company firewall to be deployed without monitoring the employee's personal activity, reduces troubleshooting when connectivity fails, and can help clarify expectations of privacy over the circuit.

Firewall Trade-offs at Home

Adding a company firewall to a previously open home network can occasionally interfere with consumer applications, a common example being Network Address Translation (NAT) compatibility messages during online console gaming. Pairing a remote firewall with a dedicated, company-paid circuit avoids most of these frictions, at the cost of some added support from time to time.

© 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.