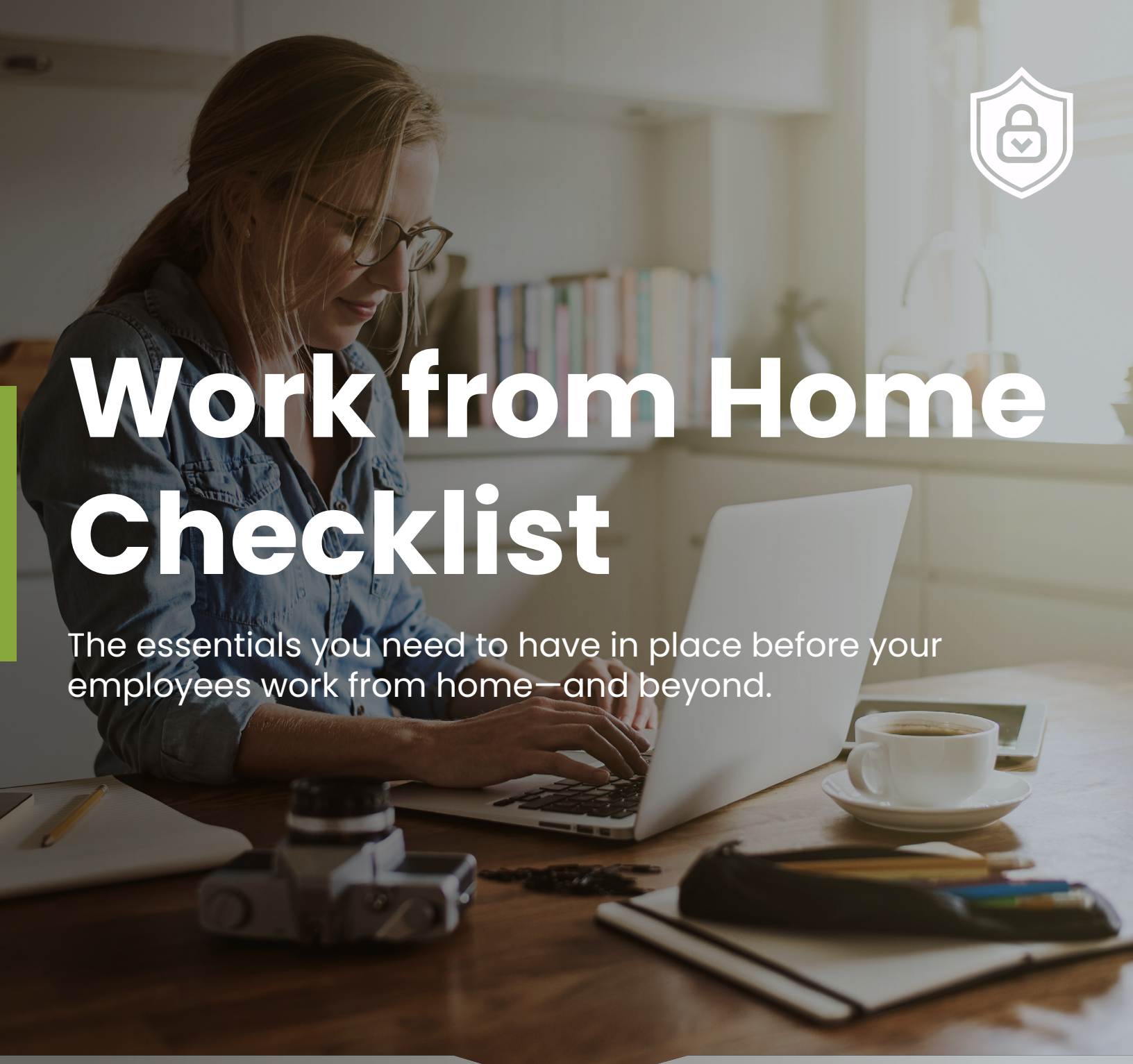


Work from Home Checklist

The essentials you need to have in place before your employees work from home—and beyond.

Managed IT | Co-Managed IT | Cybersecurity

ANDERSON TECHNOLOGIES

A Checklist by Anderson Technologies, a St. Louis IT Company

info@andersontech.com | andersontech.com | 314.394.3001 | © 2022 Anderson Technologies

Telework, Remote Work, or Work from Home

No matter what you call it, the need for remote work cybersecurity guidelines has become more urgent than ever. As world events pushed a rapid shift to employees working from home, many businesses discovered that remote work is a productive, sustainable option for their employees.

What are the risks of a remote workforce?

Remote work technology allows for interconnected workers and collaboration from abroad, but it also creates technology vulnerabilities that affect your entire business's network environment. Unless every endpoint is secured, your remote workers might be opening the door for cyber-criminals to make themselves at home.

Some businesses may feel that the flexibility of remote work is a fair tradeoff for cutting corners when it comes to cybersecurity, but this is not the case. Whether you've got an entire workforce on the go or you're trying to decide if remote work is a good long-term fit for your business, it's important to maintain the same cybersecurity standards you have with your brick-and-mortar office space.

We've created this guide as an overview of the safeguards your business needs to create a secure remote work environment. This guide prioritizes these cybersecurity measures to help you decide what best suits your business's needs.

Do Not Work from Home Without...

☐ Comprehensive Training

All employees should be routinely trained by IT professionsals on cybersecurity best practices and evolving cyber treats.

☐ Multi-Factor Authentication

Multi-factor authentication (MFA), also known as two-factor authentication (2FA), is the best protection against compromised or weak passwords. Enable it whenever it is available, and only use remote access software that has MFA capabilities. Consider MFA apps like Microsoft Authenticator, Google Authenticator, Authy, or Duo.

☐ Maintaining Updates

Make sure all computers—both in office and at home—have up-to-date operating systems with all security patches installed.

The Risk of BYOD

Not all work-from-home solutions are equal, so make sure you choose a hardware solution that ensures remote security. **Company-owned and configured devices for every remote employee will always be the safest approach;** however, not all businesses can implement this type of remote setup. If your business requires a bring your own device (BYOD) option, remember that BYOD requires additional security measures to reach the same level of protection provided by a company-owned device.

Must Haves

☐ Strong Passwords

Enforce strong password policies with a minimum of 12 alphanumeric characters that are updated at least once a year and are unique to each application.

☐ Hardware Passwords

Ensure that all home hardware (routers, modems, etc.) has WPA2-or-higher protection paired with a strong, unique password.

☐ Anti-Virus/Malware Software

Up-to-date antivirus/anti-malware software is essential for a remote setup. If employees use their home computers, maintain the limited defenses that they do have.

☐ Least Privileges

Reduce the permissions for all work-from-home employees to the minimum access necessary to perform their job. This minimizes the risk that confidential accounts and data will be compromised by an infected workstation.

☐ Administrator Access

Never allow anyone to have administrator privileges on a company-owned device. Restrict access to administrator profiles to IT professionals and only use when necessary.

☐ Hardware Inventory

Document any hardware that leaves the office and keep it maintained by the office's IT staff.

No IT system is 100% secure from breaches. All it takes is one wrong click to infect a network.

☐ Session-Locking

Implement session-locking on all remote access sessions to prevent anyone in the home besides your employee from coming upon an unattended computer and infiltrating the network.

☐ Encryption (Mobile Devices)

All company-owned mobile devices, including phone and laptops, should be encrypted in case of loss or theft.

☐ Cybersecurity Insurance

Cybersecurity insurance will help cover the costs associated with a breach, but be careful. Many policies have stipulations on the security measures required in order for the insurance claim to be paid. Failure to meet those requirements could leave you high and dry in an emergency.

Would Be Nice

☐ Company-Owned Hardware

Company-owned and maintained devices ensure that all computers connecting to the business's network are up to date and have the appropriate enterprise-level security software. Employees who regularly spend time working both remotely and in-office should consider using a company-owned laptop with a dock at their office workstation as the most efficient and secure solution.

☐ IT Configuration

Have an IT professional review and properly configure home firewalls, routers, and anti-virus/malware to shore up any holes in the home security.

☐ Password Managers

Password managers make creating strong, unique passwords easy. They store passwords in a secure vault and can generate random alpha-numeric passwords of any length, which avoids employees reusing easily-compromised passwords.

☐ Separate Profiles

If an employee must use a personal computer, create separate, password-protected user profiles that are used exclusively for connecting to the office network.

☐ Mobile Device Management (MDM) Software

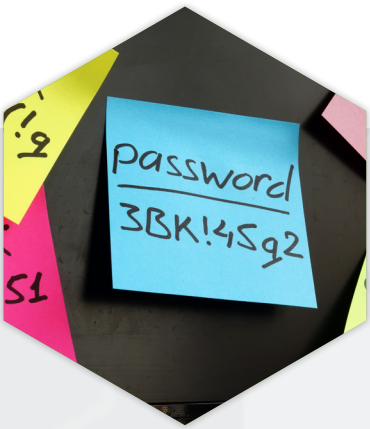
MDM software allows extended control features to be implemented on mobile devices (phones, tablets, etc.). Management controls, such as device locators and remote wipe capabilities, can minimize the risk of a breach should the device be lost.

☐ Browser Options

Limit or restrict browser plugins to only those essential for performing job functions. If on a less secure personal device, use two separate browser applications for work-related and non-work-related computer usage.

☐ Direct Virtual Private Network (VPN)

Create a direct VPN connection to the office using an enterprise-grade firewall. This will extend the office firewall and other security measures. Use a VPN connection only on a company-owned device.



ANDERSON TECHNOLOGIES

Would Be Nice (cont.)

☐ Secure Physical Documents

Any company data on physical documents should be kept in a secure place, such as a locked drawer or safe. Anything that needs to be disposed of should be shredded, not thrown away.

☐ Encryption (Home)

While working on personal devices isn't recommended, hard-disk encryption of personal computers adds an extra layer of security to the home network, especially if company data is stored on personal devices.

☐ Email Filtering

Email filtering services scan incoming and outgoing emails for dangerous attachments or links, reducing the risk that phishing emails get through to or are sent out from company emails.

☐ Voice Over IP (VoIP) at Home

If using a VoIP phone solution at the office, consider sending employees home with VoIP hardware, which only requires a power source and an internet connection.

☐ Hardware Firewalls

Provide portable hardware firewalls to all work-from-home employees to expand your enterprise-grade security measures to the home. Some vendors offer hardware firewalls that auto-connect to office networks.

It takes dogged diligence to keep your business network safe with a remote workforce.

ANDERSON TECHNOLOGIES

If You Can

☐ Locking Cables

Use locking cables to physically secure laptops whenever you are in an untrustworthy place, such as hotels or conference areas.

☐ Private Network

Establish a separate, external network dedicated to remote access. This will keep a potentially-infected home computer from compromising the entire company network.

☐ End-Point Detection and Logging

Add end-point detection and response or remote access logging to your security framework to monitor what is happening on your IT systems and catch problems as soon as they happen.

While employees may have been able to BYOD during an emergency work-from-home period, **planning for a long-term hybrid approach should include upgrades to necessary hardware.** For employees who spend time both remote and in the office, a company-owned laptop with a dock in the office extends enterprise-security effectively and removes many of the risk-introducing variables of BYOD.

While working from home may be an option for some businesses, others may need to have employees in the office at times. If you want to offer more flexibility without going fully remote, consider a hybrid model which usually involves a laptop. You can read more about the differences between a remote model and **a hybrid model** on our website.

ANDERSON TECHNOLOGIES

We hope this checklist provides a starting point for all your work-from-home needs. Moving to a new working environment can feel daunting at first, but through careful planning, comprehensive training, and proper configuration, your business can maintain a secure IT infrastructure.

Don't cut any corners on your cybersecurity needs. All it takes is one wrong click or unpatched vulnerability to infect your entire business network. Working from home doesn't have to lead to business compromise when done right.

Have any questions about working from home?

If you want to shore up your cybersecurity for a remote workforce, having access to a team of experienced IT professionals could be exactly what you need.

Anderson Technologies has been helping St. Louis businesses handle their IT needs for over 25 years. We know that running a small business means your needs are constantly changing. If you'd like to learn more about what we can do for your business, give us a call. We'd love to help remove your business's limitations.

Managed IT | Co-Managed IT | Cybersecurity