ANDERSON TECHNOLOGIES

Work from Home Checklist

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

The novel coronavirus pushed the need for a remote workforce into the public eye and with it came a rapid shift to employees working from home. With vaccine distributions beginning, some employees will return to the office, but businesses may have also found that a remote workforce is a good, sustainable situation. No matter how many employees stay at home, this Work from Home Checklist offers a quick overview of the security safeguards your business needs to create a secure remote work environment.

We've prioritized these security measures to aid you in choosing those most suited to your business's budget and needs. No matter the category, all

Do not work from home without...

Comprehensive Training

All employees should be trained by IT professionals routinely on cyber security best practices and evolving cyber threats.

Multi-Factor Authentication

Multi-factor authentication 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.

Maintaining Updates

Make sure all computers, in office and at home, have the current version of the operating system, up to date with all security patches.

Must Haves...

Strong Passwords

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

Hardware Passwords

Ensure that home hardware (routers, modems, etc.) should have WPA2 or higher password protection with strong, unique passwords on each.

Anti-Virus/Malware

Up-to-date anti-virus/malware software is essential for a work-from-home setup. Home computers have fewer protections than a business, so keep the defenses they do have maintained.

Hardware Firewalls

Provide portable hardware firewalls to all work-from-home employees to expand your enterprise-grade security measures to the home.

Least Privileges

Review and reduce all WFH employees to the minimum access necessary to perform their job. This keeps contact with confidential accounts and data to a minimum.

Administrator Access

Never allow anyone to have admin privileges as part of their everyday user account. Admin user profiles should be restricted to IT professionals for company-owned devices.

Encryption (Mobile Devices)

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

Session Locking

Implement session-locking on all remote access sessions to prevent those in the home who shouldn't have access from coming upon an unattended computer and infiltrating the network.

Cyber Security Insurance

Cybersecurity insurance will help cover the costs associated with a breach, but many policies have stipulations on the security measures required in order for the insurance claim to be paid.

Should Haves...

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.

Direct VPN

Create a direct VPN connection to the office using an enterprise-grade firewall. This will extend the office firewall and other security measures.

MDM Software

Mobile device management software allows extended control features over mobile devices, such as device locators and remote wipe capabilities for use in the event the device is lost.

Separate Profiles

Have employees using personal computers create separate, password-protected user profiles that are used exclusively for remote connecting to the office network.

Browser Plugins

Limit or restrict browser plugins only to those essential to performing job functions. When reasonable, use a different, secure browser for remote sessions.

Secure Physical Documents

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

Encryption (Home)

Hard-disk encryption of personal computers add 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 risky attachments or links, reducing the risk that phishing emails get through or are sent out using company emails.

If You Can...

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.

Private Network

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

End-Point Detection

Add end-point detection and response or remote access logging to your security framework to monitor what is happening on your IT systems.

Locking Cables

Physically secure laptops with locking cables in any untrustworthy place, such as hotels or conference areas.

We hope this checklist has provided a starting point for all your work-from-home needs. Moving to a new working environment can feel daunting in the beginning, 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 un-patched vulnerability to infect your entire business network. Working from home doesn't have to lead to business compromise when done right.

ANDERSON TECHNOLOGIES

About Anderson Technologies

We hope you found this Work From Home Checklist useful. Getting started is often the hardest part of any project, but with a little help you can have a secure remote workforce.

Have any questions?

The team at Anderson Technologies is available to discuss any questions you have or schedule a time to go over your work from home implementation needs. Contact us about our IT services today at info@andersontech.com or 314.394.3001. We're here to help!

Schedule A Free Consultation Today!

andersontech.com | info@andersontech.com | 314.394.3001