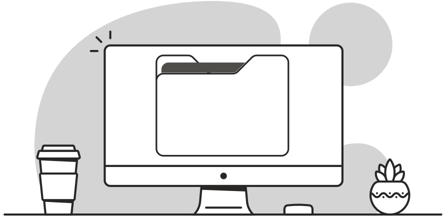
Home Networking and Bring Your Own Device (BYOD) Security Overview

A home networking and Bring Your Own Device (BYOD) checklist to ensure your users and data are protected

XTERRA



Content

How to use your checklists 3

Home Networking and Bring Your Own Device (BYOD) Security Overview 4

Home Networking and BYOD Security Checklist 6

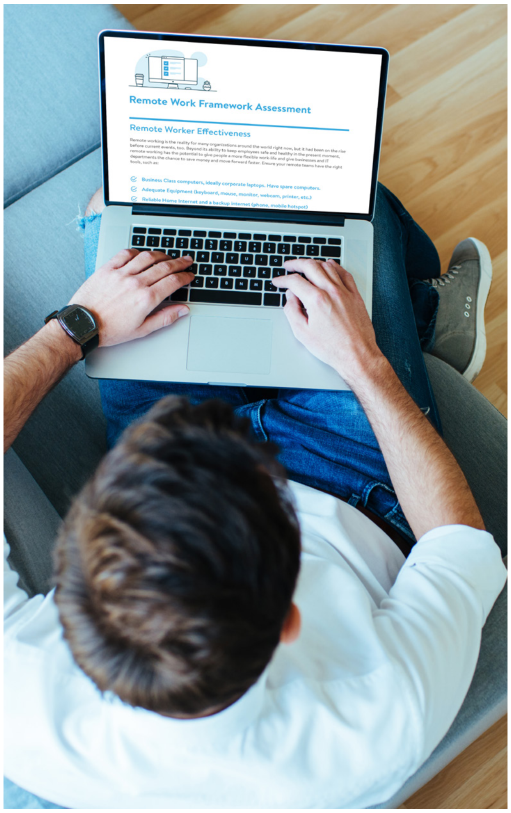
You've completed your checklists, now what? 13

We're Xterra 14

References: This document was created with guidance from the National Institute of Standard and Technology (NIST) publication: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

How to use your checklists

There’s never been a more critical time to ensure your remote workers are effective and secure.



Remote Work Framework Assessment

Remote Worker Effectiveness

Remote working is the reality for many organizations around the world right now, but it had been on the rise before current events, too. Beyond its ability to keep employees safe and healthy in the present moment, remote working has the potential to give people a more flexible work-life and give businesses and IT departments the chance to save money and move forward faster. Ensure your remote teams have the right tools, such as:

- ✓ Business Class computers, ideally corporate laptops. Have spare computers.
- ✓ Adequate Equipment (keyboard, mouse, monitor, webcam, printer, etc.)
- ✓ Reliable Home Internet and a backup internet (phone, mobile hotspot)

Get smart, get empowered, get going.
We believe it’s pretty simple; knowledge is power. We’re providing this checklist to start you on the path of validating work-from-home employees for efficacy and security. The rush to telework left many companies with their assets exposed and their staff vulnerable to attack.

Intentionally create a resilient framework.
The COVID-19 pandemic is a sobering example of the predictable nature of unpredictable events. Extended telecommuting is here to stay beyond Shelter In Place strategies – a new normal is emerging. So let’s leverage this most challenging chapter in our story to do whatever it takes to transform our organizations into inspiring examples of resiliency that can weather this crisis and future unknowns.

Know that you’re part of a local community.
Xterra has proudly served the San Francisco community with innovative IT Managed Services for over ten years. This is our home, you are our neighbors, and we intend to respond accordingly by doing whatever we can to keep local business networks, infrastructure, and teams up and running.

Need immediate assistance? We’re here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

Home Networking and Bring Your Own Device (BYOD) Security Overview

Working from home is the new normal for those of us fortunate enough to telework.

Organizations may or may not have had policies and controls in place before the COVID-19 imposed Shelter-in-Place. Malicious cyber threat actors have increased attacks on home networks, and the next battleground for your organization's data is in your home and on your devices.

Many home users share two common misconceptions about the security of their networks:

1. Their home network is too small to be at risk of a cyberattack
2. Their devices are "secure enough" right out of the box

You can increase your security to better protect yourself from these threats. The primary threat against most telework devices is malware. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and bots. Malware threats can infect devices through many means, including email, websites, file downloads and file sharing, peer-to-peer software, instant messaging, and social media. Another common threat against telework devices is loss or theft of the device. Someone with physical access to a device has many options for attempting to view or copy the information stored on it.

These guidelines are helpful for any home network or computing device. Whether working from home (WFH) is new to you or not, the following checklist should help improve your overall security and is written to share with family and friends. That said, regardless of how many security protections are used, it is simply impossible to provide 100 percent protection against attacks. A realistic goal is to use these security protections to give attackers as few opportunities as possible.

Some background before we begin:

Before implementing any of the recommendations or suggestions here, back up all data and verify the validity of the backups. Every environment is unique, so changing configurations could have unforeseen consequences, including loss of data and loss of device or application functionality.

Before teleworking, you should understand not only your organization's policies and requirements, but also appropriate ways of protecting the organization's information that you may access. You should not connect any BYOD devices to an organization's internal networks without explicit permission to do so.

You may want to perform remote access from unknown devices, such as checking email from a kiosk computer at a hotel or from a friend's mobile phone. However, you may not know if such devices have been secured correctly or if they have been compromised. Consequently, a you could use a device infected with malware that steals your information (e.g., passwords, email messages, and other sensitive data). It is generally recommended to avoid the use of kiosk computers altogether.

Safeguarding technology solutions can only go so far – it can't prevent information from being freely given away. Be alert and guard confidential information. Deception is successful because scams are convincing. Keep on guard and maintain privacy of your personal and organizational information.

Implementing the following recommendations should help you improve the security of your devices. Some of the recommendations may be challenging to implement, so seek expert assistance if you are unsure of how to implement these recommendations.

Home Networking and BYOD Security Checklist

Securing Information

Basic information security starts with the information stored on or sent to or from telework devices.

- ✓ Use physical security (don't leave laptops unattended or in the back seat of your car)
- ✓ Use Multi Factor Authentication (MFA) to access all corporate resources, email, cloud applications, and data
- ✓ Encrypt files (on computers, flash drives, etc.)
- ✓ Back up information and secure the backups
- ✓ Destroy information when it is no longer needed
- ✓ Erase information from lost or stolen devices
- ✓ Be alert for social engineering threats
- ✓ Report security breaches

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

Securing Networks

An essential part of telework security is applying these measures to networks outside of the office. Ensure that the home network is secured correctly, be cautious about allowing others to place devices on your network, and be careful when using 3rd party networks such as those in airports, hotels, or coffee shops.

Some recommendations may be challenging to implement. Follow the manufacturer's instructions on securing network devices and seek expert assistance when unsure how to proceed.

Wired Home Networks

Secure your home network by separating your internal home network from the external network of the Internet Service Provider (ISP) as much as possible. Connecting directly to the ISP, such as plugging a device directly into a cable modem, exposes the device directly to the Internet. This is a very high-risk vector of attack.

- Use a broadband router (e.g., cable modem router) or a physical firewall appliance
- Change the default password
- Block administration from outside the home network
- Apply updates automatically or at least monthly if set to manually update
- Configure the device to ignore unsolicited ping requests
- For broadband routers, disable the built-in wireless access point if not used

Wireless Home Networks

Wireless Access Points (WAPs) are a common way to connect devices, both personal and telework, at home. If improperly configured, a wireless home network will transmit sensitive information and expose it to other devices in proximity of the signal.

- Upgrade firmware and turn on automatic updates
- Use strong encryption – WPA2 or WPA3 with AES (do not use WEP)
- Make your WPA2 key long and complex
- Change the default SSID (the "network name" associated with your WAP)
- Set up a guest Wi-Fi for visitors, do not share your internal network information
- Disable Wi-Fi Protected Setup (WPS)
- Disable Universal Plug and Play (UPnP) when not needed
- Disable SSID broadcasts (hide the SSID)
- Disable AP administration through wireless (remote management)
- Reduce wireless signal strength to your home's boundaries

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

External Networks

External 3rd party networks (hotel rooms, coffee shops, etc.) other than home and work are the least protected. Assume these networks have insufficient protection for your devices.

- ✓ Ensure your device OS is updated and patched
- ✓ Establish a VPN session immediately after connecting to the 3rd party network

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

Securing BYOD Computers

✓ Software Updates

Many threats take advantage of vulnerabilities in software on computers. Software manufacturers release updates to eliminate these vulnerabilities. Ensure that updates are applied regularly to the major software on your computers.

Microsoft and Apple generally support security updates of their software within two versions of the current Operating System (OS).

Microsoft Windows

- ✓ As of this writing, this includes Windows 10 version 1809 which reaches End of Service in November 2020
- ✓ https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

Apple macOS

- ✓ As of this writing, this includes High Sierra which reaches End of Life in September 2020
- ✓ https://en.wikipedia.org/wiki/MacOS_version_history

In addition to the OS, updates should include standard software. Review manufacturer documentation to determine your update capabilities. Enable features to check for updates automatically and keep programs up to date weekly – even more frequently for security software such as antivirus. For programs that do not offer automatic updates, run the update feature from the application's menus every week, and install any available updates:

- ✓ Web browsers
- ✓ Email clients
- ✓ Instant messaging clients
- ✓ Office productivity software (word processors, spreadsheet tools, etc.)
- ✓ Antivirus software
- ✓ Personal firewalls

✓ User Accounts

User accounts (your login account) can have full or limited privileges. Administrative accounts (full) should only be used for management tasks such as updates or managing user accounts. If your computer is attacked while an Admin account is in use, the attack can do more damage. Therefore, use a daily use (limited) account for routine tasks such as reading email, web browsing, and social networking, because these tasks are a common way to infect computers with malware.

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

Every account should be protected

- Use a long password (8 characters or longer)
- Make the password complex (upper and lower case, digits, and symbols)
- Avoid similar passwords
- Do not use password hints
- Do not repeat passwords for other accounts – use a password manager
- Protect your session from unauthorized physical access – use a screensaver lock timer

Limit some Networking features

- Disable unneeded networking features such as IPv6
- Limit the use of Remote Access utilities
- Disable ad hoc networking (computer to computer)

Prevent Attacks

- Open and execute files only from trusted and known sources
- Install and use only trusted and known software
- Install and configure Antivirus software
  - Automatically check for updates at least daily
  - Scan critical OS components such as startup files
  - Monitor the behavior of common apps such as email and web browsers
  - Perform real-time scans of files
  - Scan all hard drives regularly
  - Scan removable media
  - Handle infected files by attempting to disinfect or quarantine the files
  - Log all significant actions such as scan results and discovered malware
- Use a personal firewall
  - Enable the personal firewall in the OS or use a 3rd party software firewall on your computer
  - Log all significant actions such as blocked activity and configuration changes
  - Ideally, personal firewalls should deny all types of communication that are not explicitly approved (deny by default)
- Practice safe web browsing
  - Use web content filterings such as OpenDNS or Cloudflare
  - Use a different brand of browser for teleworking (Internet Explorer/Edge, Safari, Chrome, Firefox, Opera, etc.) than standard web browsing to limit malicious content or spyware plug-ins to a single browser

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

  - Block pop-up windows
  - Enable phishing filter capabilities in the browser
  - Remove unneeded browser plug-ins
  - Password protect sensitive information stored by the browser such as passwords and certificates
  - Disable autofill and autocomplete in the browser
- Email client safety
  - Use a spam filter
  - Do not click unknown or untrusted links or attachments
  - Set default reading format to plain text
  - Disable automatic previewing and opening of email
- Instant Messaging safety
  - Suppress the display of email addresses
  - Restrict file transfers
- Office Productivity Suite configuration
  - Restrict macro use
  - Limit personal information embedded in documents
- Limit Remote Access software – configure based on the organization’s requirements and recommendations

Securing BYOD mobile devices

Given the wide variety of mobile devices, it is not feasible to create specific recommendations to apply to all mobile devices. Therefore, teleworkers should consult the documentation provided by the manufacturer and follow their security recommendations. **General recommendations are as follows:**

- ✓ Limit access to the device by setting a complex password and don’t use the password elsewhere
- ✓ Add biometrics to the password
- ✓ Configure the device to lock after an idle period
- ✓ Disable unused networking features such as Bluetooth and Near Field Communication (NFC) except when needed
- ✓ Ensure that security updates are installed at least weekly, preferably daily
- ✓ Configure applications to support security (e.g., blocking activity that is likely to be malicious)
- ✓ Only use authorized app stores
- ✓ Do not jailbreak or root the device
- ✓ Avoid unknown charging stations and computers
- ✓ Install the Mobile Device Management software from your organization, if available
- ✓ Use an isolated and encrypted environment to access the organization’s data and services

Need immediate assistance? We’re here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

You’ve reviewed your checklists, now what?

It’s all about creating momentum. Here’s what you can do now.

Raise awareness

Get out of overwhelm and turn anxiety into decisive actions.
Even though the checklists you’ve reviewed are comprehensive and represent a substantial amount of effort, they are, by definition finite, and therefore doable. Thus just getting familiar with these items is an essential first step.

Inform your team

Get your team aligned, focused and executing.
Use these checklists to drive an essential internal meeting with your staff to assess where you’re at as an organization, get feedback, and begin the process of delegating effort to the items that have revealed themselves to be most critical.

Secure yourself

Malicious cyber actors are exploiting COVID-19.
The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a joint alert (AA20-099A) that the surge in teleworking has increased the use of potentially vulnerable services and has amplified the threat to individuals and organizations.

Engage with Xterra

Take advantage of our free 20-minute consultation.
To the best of our ability, we’re here to help. So if you have some urgent issues or have any followup questions regarding the checklists, you can schedule a free 20-minute consultation by emailing solutions@xterrasolutions.com.

Need immediate assistance? We’re here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

We're a local and trusted technology resource

Data and technology security is a critical and ongoing agenda for Xterra.

As your both your remote and local San Francisco neighbor, we're here to help ensure the business resiliency you and your team need–today and beyond. As the current COVID-19 lockdown painfully illustrates, having a well-defined remote worker security strategy is more critical than ever. Xterra has served the local San Francisco business community for over 10 years, delivering innovative IT Managed Services to provide predictable cost management; prudent, responsive budgeting; and secure employee productivity.

Xterra delivers solutions that fit your specific needs, including:

MANAGED SERVICES

- IT Service Desk
- Infrastructure Management
- VoIP Solutions
- Virtual CIO Services
- Vendor Management
- Hardware as a Service
- Security and Compliance

CLOUD SERVICES

- Microsoft Cloud
- Virtual Server Hosting
- Cloud Monitoring
- Secure File Sharing
- Backup and Recovery
- Server Colocation

SPECIALIZED IT

- IT Consulting
- Virtualization
- Enterprise Wireless Solutions
- Structured Cabling Solutions
- Migration and Deployment
- Office Moves

In response to the unprecedented circumstance we find our community in, we're scheduling free 20-minute consultations to help problem-solve your unique challenge. During this call, we can help you prioritize your agenda, help you tap into resources that may be available to you, or provide any feedback or guidance as it relates to the checklists you just reviewed. San Francisco is our city, and you're an essential part of that community, let us know how we can help. To schedule your free 20-minute consultation, please email solutions@ xterrasolutions.com. If you have a more urgent issue, you can call us at 415-844-9730. Stay safe, determined, and resilient.

> "**Xterra exceeded all expectations during the COVID-19 lockdown as our firm transitioned from office to working remotely in a matter of hours.** Before we anticipated the need, and at lightning speed, the company pivoted to become our work at home nerve center. Xterra prepared a security checklist and educated our staff, town-hall-style, on how to work securely from home. The CEO even hand-delivered a Wi-Fi hotspot device to an employee in need of a stronger internet connection. This is the kind of support one wants, especially in a crisis."
>
> **- John Ashworth, Principal**
> AIA, LEED AP, NCARB
>
> bull stockwell allen
> ARCHITECTURE + PLANNING + INTERIORS

Need immediate assistance? We're here to help. Call us at **415-844-9730** or email us at **solutions@xterrasolutions.com**

XTERRA