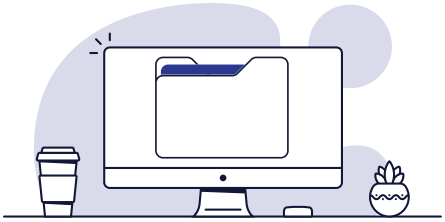
Ensuring your remote worker framework is effective and secure

A checklist for your COVID-19's
Work from Home reality and beyond.

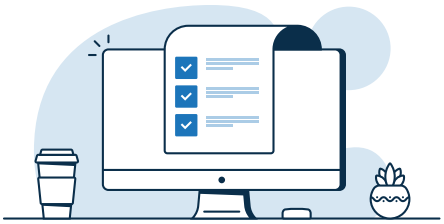
XTERRA



Content

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.800-46r2.pdf

XTERRA



How to use your checklists

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

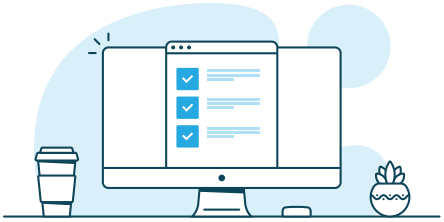
Get smart, get empowered, get going.
We believe it's pretty simple; knowledge is power. We're providing this checklist to start you on the path of validating work-from-home employees for efficacy and security. The rush to telework left many companies with their assets exposed and their staff vulnerable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

XTERRA



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. Beyond the ability to keep employees safe and healthy in the present moment, remote working has the potential to give people a more flexible work-life balance 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:

Home Office Infrastructure

- Business Class computers, ideally corporate owned laptops. Have spare computers.
- Adequate Equipment (keyboard, mouse, monitor, webcam, printer, etc.)
- Reliable Home Internet and a backup internet (phone, mobile hotspot)
- Home Network is patched and WiFi is configured for WPA2 encryption
- Ergonomic Home Office setup (desk, chair, lighting, noise reduction, etc.)
- Office Phone is available remotely (softphone, multi-ring, or call forwarding)

Remote Worker Applications

- Productivity Application such as Office 365 or G Suite
- Video Conferencing with screen sharing (Zoom, WebEx, GoToMeeting, etc.)
- Team Collaboration Application (Slack, MS Teams, etc.)
- Secure File Share & Sync (Egnyte, OneDrive, Box, etc.)
- Line of Business Applications are securely available

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

XTERRA

Remote Access & Service Discovery

Inventory how people connect to internal resources and the resources they require for remote work.

List Methods to Access Company Resources

- Virtual Private Networks (VPN)
- Web-based portals, terminal servers, or virtual desktop infrastructure (VDI)
- Computers available using a Remote Desktop application
- Applications accessed directly through a network DMZ
- Corporate Virtual Machines (VMs) used on Bring Your Own Device (BYOD) computers

Inventory Internal Applications

- List internal applications that are required to work remotely
- Assign applications an “owner”
- Create provisioning & termination checklists for access to applications

Inventory Cloud Services

- List cloud services
- Assign services an “owner”
- Create provisioning & termination checklists for access to services

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

XTERRA

Remote Access Security

The security of remote access methods is crucial because they provide a way for external parties to gain access to internal resources. Organizations can use multiple remote access solutions if users have different security needs. The most common security objectives for telework and remote access technologies are confidentiality (access to authorized parties only), integrity (detect changes to data), and availability (users can access required resources).

Datacenter security and performance

- Datacenter hardware (firewall, switching, servers) is in place and redundant
- Network failover (alternate carrier/ISP) is working and Carrier contact information is available
- Performance is adequate for your entire remote workforce (High speed, 100 Mbs+, Symmetrical)
- All equipment is on a monitored uninterruptable power supply (UPS)

Network topology and traffic inspection

- Firewall is inspecting traffic (including SSL encapsulated traffic) and blocking unauthorized traffic
- Untrusted geo-locations (North Korea, Iran, etc.) are blocked
- VPN uses full tunnel (no split tunnel internet) to prevent untrusted home or public networks connecting to internal resources
- Intrusion Prevention System (IPS) in place
- DNS Filtering in place (OpenDNS, Webroot, Cloudflare, etc.)

Authentication

- Identity Management System in place (Active Directory, Jumpcloud, Okta, etc.)
- Password Management System in place (Secret Server, Centrify, LastPass, etc.)
- Certificates are used to verify identity
- Multi-factor Authentication (MFA) is used across all logins

Authorization

- Health checks are performed for authenticated devices
- User and System access is limited using privilege model

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

XTERRA

Encryption

- Network traffic data is encrypted in motion (sent/received)
- Data is encrypted at rest (when stored)
- Disk encryption is managed for all corporate systems
- Email encryption is available for confidential corporate data
- Encryption certificates are securely stored and backed up

Logging

- Devices, systems, and applications are configured to log important events such as access control and privilege elevation
- Logs are forwarded to a Security Incident Event Management (SIEM) such as AlienVault, Splunk, or 3rd party service

Operations and Maintenance

- Policies are documented and reviewed regularly
- Data, applications, and configurations are backed up and tested
- Assets are known, managed, and patched
- Systems are configured to best practices instead of default settings
- Central monitoring and alerts are set up
- Regular technology assessments and audits are performed

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

XTERRA

Secure Client Devices

Define which devices are allowed access to data and how they should be configured. This includes company owned and Bring Your Own Device (BYOD) computers and mobile devices. Malware, loss, and theft remain threats to everyone.

Computers

- Complex passwords are used
- Network and Personal Firewalls are turned on
- Applications are known and updated (software is inventoried)
- Identity Management is in place
- Endpoint security is up-to-date for antivirus/antimalware/next generation security

Mobile Devices

- Complex passcodes are used
- Rooted or “jailbroken” phones are not allowed
- Mobile Device Management is in place (Intune, Airwatch, Jamf, etc.)

Both Computers and Mobile Devices

- Operating Systems are up to date and patched
- Screen locking (session locking) is configured
- Minimal corporate data is stored on local systems
- Data is encrypted at rest (when stored)
- Disk encryption is managed for all corporate systems and encryption keys are available for recovery
- Corporate data is backed up
- Data can be destroyed or locked remotely when no longer wanted/needed on the device

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

XTERRA

Remote Access Policy and Training

Identify current and future needs; specify requirements for performance, functionality, and security. Be sure to plan telework-related security policies and controls based on the assumption that external environments contain hostile threats; that devices are prone to loss, theft, and malware; and that communications on external networks are susceptible to eavesdropping, interception, and modification. Train your workforce for working remotely.

Define permitted forms of remote access (VPN, Cloud, VDI, etc.)

Determine restrictions on Client Devices and Remote Access levels

- Evaluate acceptable risk and your budget for solutions
- Know the sensitivity of your data such as intellectual property; trade secrets; and Personally Identifiable Information (PII) (Social Security numbers, home addresses, credit card numbers, etc.)
- Set approved telework locations (home office, internet café, international travel)
- Mitigate or accept technical limitations (application limitations, custom office procedures, workflow restrictions that prevent telework)
- Understand compliance with mandates, external policies, and legal guidelines (PCI, HIPAA, Fed/State/Local laws, etc.)

Create and Manage your Policies

- Create security policies to mitigate risk and to document approved remote access methods and devices
- Establish Bring Your Own Device policies for computers and mobile devices
- Evaluate policies on a recurring basis and document security decisions
- Review Operational processes – updating systems, adjusting access, and documenting anomalies
- Document how to retire devices and wipe sensitive data properly

Educate Users

- Provide Security Awareness Training and social media guidance
- Remote Access Methods, Security, and Policy
- Education is available Teleworking Applications (Web conferencing, Team Collaboration, Document Storage, etc.)
- Set Communication expectations with employees working remotely

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

XTERRA

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**

XTERRA

We're a local and trusted technology resource

"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

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 business continuity and 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 uniques 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.

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

XTERRA