



WFH and Hybrid Work: How to Stay Secure In 2022




WFH and Hybrid Work: How to Stay Secure In 2022

Any work done outside of the office increases the risk to your systems.

Regardless of whether your company has employees who Work From Home (WFH), Work From Anywhere (WFA), or a combination of WFH/WFA and the office (hybrid), everyone needs to work together to keep your company safe. When you, your employees, and your IT department all do their part, your organization can steer clear of most breaches, malware, ransomware, unauthorized device and network access, social engineering, the temptation to use workarounds, and other threats.

Required hands-on training with continuous testing of all employees at every level, including leadership, turns talk into action.



If your company must comply with regulations, the stakes are even higher. Forward-thinking companies follow compliance-ready security policies even if they aren't regulated because secure companies win more business.

The best way for your company to stay secure is for everyone to do everything right every time. Tall order? It's doable! Here's the best way to get as close as possible.

What your employees need to do: Adhere to your policies

As your most important firewall, your employees should understand your policies inside out so they can follow them. Policies need to be written, practiced, and overseen. The more you emphasize the importance of security to your business (and their jobs), the more effort they'll make.

Required hands-on training with continuous testing of all employees at every level, including leadership, turns talk into action. Security awareness training from companies like [KnowBe4](#), [PhishLabs](#), [Cofence](#), and [Proofpoint](#) test employees after they complete the training modules. The training programs also require employees to officially acknowledge they've completed the training and understand what's expected. You can follow up with additional random testing and internal phishing tests to see which, if any, of your employees are still vulnerable.

Finally, make sure every employee signs off on your policies regularly and whenever you make a policy change.

What leadership needs to do: Set up your employees (and company) for success


Leadership's role is to protect your company while making it easy for employees to comply. These six steps can guide you:

1. Update your Cybersecurity (or Compliance) Policy for remote working

- Write your policy in clear language — avoid a bone-dry presentation — and make sure it's board-reviewed and available on your intranet for easy access and quick reference
- Include your approved systems, apps, and any external media (like flash drives and hard drives)
- Define the types of information that must always stay on the company network and the process for sending approved sensitive information
- Write specific requirements for multi-factor authentication (MFA), password, and encryption, including your processes for communications, data storage, wireless routers, and router traffic
- Incorporate a Media Sanitization Policy that covers the disposal of sensitive information, including hard copies, if needed
- Other policies you may want to integrate or update include:
 - Security Awareness Training Agreement
 - Confidentiality Agreement
 - Bring Your Own Device (BYOD) Agreement
 - Sanction Policy

2. Task your IT department with updating or upgrading your IT environment for remote working (see details in the next section)

Write your policy in clear language — avoid a bone-dry presentation — and make sure it's board-reviewed and available on your intranet for easy access and quick reference



3. Engage a reputable training company if you haven't already

- Choose a company that makes learning interesting and engaging — subpar or boring training modules don't encourage learning or compliance
- Determine your required time frames for completion and make completion mandatory
- Ask for feedback about the training and change training companies if your employees are dissatisfied

4. Shore up oversight, especially if you must meet compliance regulations

- If you have a compliance officer, support that role with a compliance committee
- Require monitoring and auditing (including spot-checking) of all staff and regular internal reporting
- Review and update your investigation plan and require follow-through on corrective actions and discipline
- Establish a hotline for confidential and anonymous reporting of security or compliance issues


5. Conduct employee orientations

- Inform all staff about the policy updates you're making and why
- Emphasize that your employees are your company's first line of defense, that you rely on them to keep your business operating successfully, and that it's important for everyone to work as a team
- Be clear about your training requirements and what you expect on a continual basis
- Lead by example by talking about compliance improvements you've made to your own workflow

6. Continue to talk about your security policies — a lot

- Send a strong signal at every reasonable opportunity that security (and possibly regulatory compliance) is a top priority
- Include security and compliance messaging in your internal communications
- Remind your entire team to be vigilant in looking out for scams and tell IT about anything that seems suspicious
- Congratulate your team on its successes because recognition has a positive impact

Emphasize that your employees are your company's first line of defense, that you rely on them to keep your business operating successfully, and that it's important for everyone to work as a team



What your IT department needs to do: Configure your IT environment for remote working

The key to having a compliance-ready environment is not to differentiate between “remote work” and “work” — they are now the same. Your IT department should address these three areas:

Operations

- Configure all devices with the latest software and security controls with automatic patches
- Review access logs more often and check every IP address to check for anomalies
- Monitor and test VPN limits to stay ahead of any increases in the number of users


Solutions

- Shore up remote access security practices, including implementing [MFA across the board](#) (and ideally a remote access single sign-on solution) and reviewing wireless encryption protocol, vulnerability management, digital asset protection, backups
- Leverage [zero-trust](#) or conditional-access rules
- Use tools and platforms built for a distributed workforce when moving resources to the cloud
- Look at VDI (virtual desktop infrastructure) or virtual desktops or endpoint protection software for your employees’ personal computers

Policies

- Update your runbooks to reflect any changes you’ve made to secure remote access and document any gaps you find
- If you must meet compliance standards, publish your company’s audit policy that defines what IT will be looking at to balance security and privacy

The key to having a compliance-ready environment is not to differentiate between “remote work” and “work” — they are now the same.



Security from anywhere is a business benefit

Staying secure and in compliance, regardless of where your employees do their work, is a team effort that starts at the top. By training employees on well-defined policies, having a properly configured IT environment, and continually demonstrating that security is a cornerstone of your corporate culture, the added risk of remote work is manageable.

A distributed workforce offers many advantages that can propel you forward in 2022 and beyond. By taking the steps needed to keep your systems secure, you can capitalize on the advantages without putting your business at risk.

Leapfrog Services is an IT Security, Network, and Infrastructure Managed Service Provider (MSP/MSSP) that's been helping organizations meet their business goals and protect their data since 1998. Our team designs and operates outsourced solutions based on our proven methodology that includes matching your level of threat protection to your business needs and adhering to the highest cybersecurity standards (we are SSAE 18 SOC 2 compliant). Guarding against risks systematically and consistently reduces the likelihood your organization will be attacked and helps you to remain productive and successful.

You can reach us at 404-870-2122 or [leapfrogservices.com](https://www.leapfrogservices.com).

