Ascend TECHNOLOGIES

IT SAFETY CHECKLIST:

HOW TO ENSURE YOUR REMOTE EMPLOYEES ARE SAFE

A comprehensive list to prepare your business and telework employees for remote access

CONTENTS

THE STATE OF MOBILE WORKFORCES

AND REMOTE OPPORTUNITIES

ADVANCES IN NETWORKING AND MOBILE TECHNOLOGIES HAVE ENABLED WORKFORCES TO MOVE OUTSIDE OF THE CONFINES OF THE OFFICE ON A GLOBAL SCALE.

Whether you're a small business with employees in different countries or just sick at home with the flu, remote work has become an alternative for businesses to reduce costs and enhance their employees' work/life balance. With advancements in collaborative AI tools, 5G connectivity, and the increased use of VR/AR for virtual meetings & events, working from home has never as streamlined.

- FORTUNE 1000 COMPANIES AROUND THE GLOBE ARE ENTIRELY REVAMPING THEIR SPACE AROUND THE FACT THAT EMPLOYEES ARE ALREADY MOBILE. STUDIES REPEATEDLY SHOW THEY ARE NOT AT THEIR DESK 50-60% OF THE TIME.

- OVER 45% OF THE GLOBAL WORKFORCE IN 2024 OPERATED REMOTELY, AT LEAST PART-TIME, WITH HYBRID WORK MODELS BECOMING THE NEW NORM.

WHY BUSINESSES NEED TO BE THINKING ABOUT REMOTE EMPLOYEE IT SAFETY

The trend of remote workers has become ubiquitous as a perk to attract top talent. As previously noted, most US workers expect some wiggle room with work-from-home policies.

01 **Focus on Enterprise-Level Challenges**: Emphasize the complexities of managing IT security across large, distributed teams. Highlight the need for robust security frameworks that can scale with the size of the organization, such as implementing centralized security operations centers (SOCs) that monitor and manage security across all remote work environments.

02 **Advanced Threat Management**: Discuss the importance of using advanced threat detection and response systems, like Extended Detection and Response (XDR), which are essential for large businesses that face sophisticated cyber threats.

03 **Secure Collaboration Across Multiple Locations**: Address the need for secure and efficient collaboration tools that can be used across multiple locations, including global offices and remote workers. Highlight how enterprise-level businesses can benefit from integrated collaboration suites that combine secure communication, document management, and project tracking.

04 **Data Governance and Compliance**: Stress the importance of adhering to stringent data governance and compliance regulations, which are critical for large organizations handling vast amounts of sensitive data. Mention the need for regular audits and updates to security policies to stay compliant with industry standards such as GDPR, CCPA, and HIPAA.

05 **Investing in Cybersecurity Training Programs**: Recommend that enterprises invest in ongoing cybersecurity training programs tailored to different roles within the organization, ensuring that all employees are aware of potential threats and how to respond to them. This is especially crucial for large organizations where the risk of human error can have widespread consequences.

06 **Building a Resilient IT Infrastructure**: Highlight the need for a resilient IT infrastructure that can support the demands of remote work at scale. This includes investing in enterprise-grade VPNs, cloud-based security solutions, and disaster recovery plans that ensure business continuity in the face of cyber threats or other disruptions.

COMMON RISKS REMOTE EMPLOYEES FACE

Remote employees, such as freelance workers or employees from other states or countries, are less likely to be working from company-issued devices.

If your organization does not assign and ship devices to your remote workers, then you will not be able to encrypt the devices they're using. They're also more likely to use an array of devices throughout the day, creating a moving target for your IT team to manage.

Even though your organization may have agreements with employees and third parties that require their client devices to be properly secured, those agreements generally cannot be automatically enforced, so unsecured, malware-infected or otherwise-compromised devices may end up connected to your resources.

Personal devices and migration of data also increases the odds an employee loses a device with sensitive information on it.

From thumb drives to mobile phones, mistakes happen.

REMOTE EMPLOYEE SAFETY CHECKLIST

WE'VE PACKAGED THIS CHECKLIST INTO PHASES TO HELP YOU COMPLETE THESE KEY STEPS. KEEP IN MIND, EACH TASK SHOULD BE COMPLETED BEFORE YOU ALLOW EMPLOYEES TO TELECOMMUTE.

THE QUICK LIST

- Utilize cloud-based storage for advanced encryption & real-time collaborative features
- Encrypt devices whenever possible
- Use a VPN
- Roll out automatic updates to remote devices
- Set up an encrypted email platform
- Deploy an endpoint security program
- Implement AI-based threat detection systems
- Ensure zero-trust network access (ZTNA)
- Incorporate secure access service edge (SASE) frameworks

Before deploying a remote access solution, you should test all remote access opportunities as well as available resources against a variety of threats. This will ensure you have designed a reliable system.

NECESSARY ASSUMPTIONS

While building your remote employee IT strategy, always keep in mind the following:

01 Communications on external networks are susceptible to eavesdropping, interception, and modification.

02 Networks between the remote employee's device and the organization cannot be trusted, and require continuous verification of all users, devices, and apps–both in & outside the network.

03 Eventually, your teleworkers' devices will become infected with harmful malware.

04 With more employees working in environments distributed across multiple, vast regions, accounting for scalability is crucial in remote access solutions.

GUIDELINES

HOW ARE YOU GOING TO ENSURE YOUR REMOTE WORKERS ARE SAFE?

- Create a plan to educate your employees about security and best practices.

- Develop a telework security policy that defines telework, remote access and use of personal devices.

- Establish protocols for information sharing.*

- Select an asset tracking platform to locate your remote devices and complete all the necessary paperwork.

- Create a procedure for rolling out updates to operating systems or applications for all remote devices.

- Build guidelines that define what happens to issued devices that are lost or stolen and how remote workers are to report such occurences.

- File insurance policies for remote devices in the event of theft or burglary. You may also choose to file the devices under the homeowner's insurance.

- Draft procedures for monitoring devices in the event they've been unknowingly compromised off-site and are later brought into the office and connected to your network.

**This defines what forms of remote access the organization permits, what devices are permitted and what type of access each remote worker is permitted. It should also include how the organization's remote access servers are administered and how policies in those servers are updated. You may want to create tiered levels of access to help limit risk and assign them to different users by employment level or the types of devices they use.*

COMMUNICATION PLANS

HOW WILL YOU ENSURE REMOTE WORKERS CAN SEND AND RECEIVE CRUCIAL INFORMATION?

- Have communication tools in place and select a video call platform
- Create a clear action plan for emergency announcements:

How do you communicate about emergencies at the office to remote employees?

How do teleworking employees relay that they've experienced an emergency at their work-location to you at the office?

SECURITY

HOW WILL YOU TRAIN REMOTE WORKERS TO AVOID DEVICE CORRUPTION AND PROTECT YOUR COMPANY ASSETS?

- Mandate strong passwords for work and personal accounts
- Never share credentials
- Enable two-factor authentication wherever possible
- Use a secure email platform
- Install asset tracking software
- Set remote devices to store information in cloud-based storage solutions which are encrypted and offer better protected from ransomware or malware
- Do you have remote access controls which are accessible while a user is at home? This helps with isolating device if compromised and enable routine patches for your support team
- Create a secure VPN
- Establish endpoint security program that creates safe access for all devices
- Does your firewall support multiple policies to account for unique devices?
- Apply high securities to your office and minimum restrictions for teleworkers

• Mandate user-protected locking mechanisms/locking screensaver

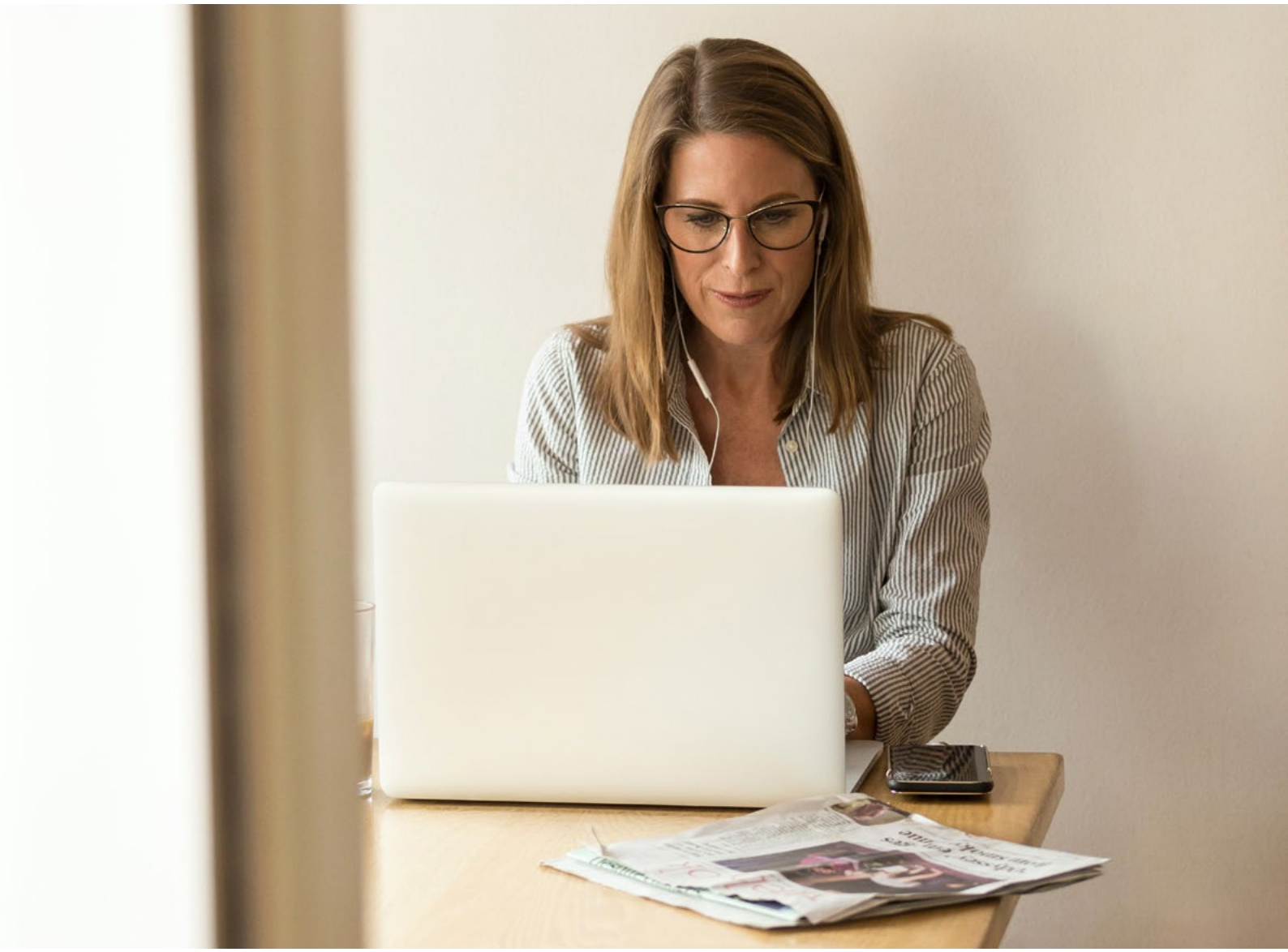
• Session locking prevents access to a device after it has been idle for a period of time.

• Require unique access codes for personal devices.

• Do not allow personal devices to connect to network firewalls.

• Limit the networking capabilities of mobile devices. This is important for devices that have multiple wireless capabilities; the teleworker might not know that some wireless protocols are exposing the device to access by attackers such as Bluetooth and shared wireless networking. You may have to allow multiple network capabilities simultaneously like voice and Wi-Fi.

• Specific device-specific encryption can save a lot of headaches, like bitlocker.



PRODUCTIVITY

HOW WILL YOU FIX A BLACKOUT OR POWER FAILURE?

- Plan to mitigate downtime in the event a user's device becomes unusable.
- How to monitor remote devices for IT needs? What plan do you have in place if a user needs IT help which requires physical access to equipment?
- How does this affect billable hours or commission-based workers?
- Plan for a teleworker who encounters ISP downtime. Do they divert to a mobile hotspot or a coffee shop? Do you overnight a hotspot device until employee service is restored?

EQUIPMENT

ACCIDENTS HAPPEN.

HOW WILL YOU PROTECT YOUR INVESTMENTS?

- Purchasing device warranties is never a bad idea. Choose the plan that best suits your budget and life expectancy of devices.
- Consider purchasing on-site service warranties, damage warranties or extended warranties for personal computers and mobile devices.
- Dell and Innova offer services where an IT specialist will show up to a remote location to fix or repair devices.
- Ascend's Digital Workplace Deployment allows you to quickly deploy devices while maintaining a consistent security standard.
- Protect your business's success with uninterrupted access to IT support and services with Ascend's 24/7 Support Desk.

If your remote employees have pets or children, it's not a bad idea to make sure help is never far away.

PRODUCTIVITY

HOW WILL YOU HANDLE DEVICES WHICH HAVE BEEN CORRUPTED OR THOSE BELONGING TO EMPLOYEES WHO NO LONGER WORK FOR YOU?

Do you have guidelines for wiping devices clean?

- **Update Device Management Practices**: With the rise of remote work, suggest using remote wiping and data retrieval technologies that can securely erase or recover data from devices no longer in use.

- **Strengthen Offboarding Procedures**: Provide detailed steps for securely offboarding remote employees, ensuring that access to company resources is immediately revoked and all company data is retrieved.

HIPAA CAVEATS

IS YOUR ORGANIZATION SUBJECT TO SPECIFIC SECURITY PROTOCOLS DUE TO YOUR INDUSTRY?

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information (e-PHI). Covered entities must:

1. Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit.

2. Identify and protect against reasonably anticipated threats to the security or integrity of the information.

3. Protect against reasonably anticipated, impermissible uses or disclosures.

4. Ensure compliance by their workforce.

5. Adhere to compliance standards relevant to various indsutries, such as GDPR for European businesses, CCPA for California-based companies, and other regional data protection laws.

ARE YOU READY FOR A REMOTE WORKFORCE?

Remote workers may provide challenges for an IT staff, but a balanced strategy that educates and empowers users can ensure your company's safety — whether employees are checking their email at a coffee shop or connecting from another country.

If you want to protect your business from attacks and penetration while your employees enjoy the benefits of remote work, you must take precautionary measures to create a secure environment.

Future-proof remote work strategies by investing in adaptable technologies and keeping pace with the rapidly changing digital landscape.

By covering the essentials and preparing for the worst, you'll be giving yourself an upperhand in the event of a disaster while providing confidence for your remote workers to protect themselves and their devices in every scenario. If you have questions, we're here to help.

Companies must remain proactive in evolving their security strategies to stay ahead of emerging threats, while ensuring seamless collaboration. By embracing innovative solutions and prioritizing both security and employee experience, organizations can create a resilient, productive, and future-ready workplace.

Ascend Technologies is a far cry from your run-of-the-mill managed services provider. Our information technology professionals help business leaders make IT investments with confidence, eliminate cybersecurity threats, meet the needs of the business, and optimize user productivity — making technology the catalyst for business expansion.