Ensure your team has a secure and productive work-from-home (WFH) environment

This self-assessment is for organizations implementing remote work IT infrastructure. It is designed to provide visibility into your readiness, from both the technical and policy perspectives.

Check each item against your organization's current status. If you are not sure of an answer, assume it is "No".

Procedure and Policy

1. Has your organization created and disseminated a WFH policy?
2. Does the policy include tracking attendance and availability?
3. Does the policy include task tracking with digital timesheets to ensure productivity is maintained?
4. Have all employees been notified of the WFH policy and given time to seek clarifications?
5. Has your organization chosen a primary method for communicating with team members?
6. Does your WFH policy include the lending of office equipment to employees in need, and an asset-tracking procedure (checkout forms, inventories, etc.)?
7. Has your organization provided training or other resources for learning to work effectively from home?

Basic Equipment

1. Do your employees have access to the following:
    1. Reliable high-speed internet?
    2. Desktop computer, laptop, or sufficiently capable tablet with peripherals?
    3. Webcam?
    4. Headset, or headphone and microphone ?
    5. Uninterruptible power supply (UPS)?
    6. Appropriate workspace?
    7. Ergonomic chair suitable for long hours of sitting?
2. Do all of your employees know how to synchronize their work data to their home computers?
3. Do your employees require additional software licenses to perform their tasks remotely?
4. Are you allowing employees to access your organization's cloud via personal devices, and if so, have you created and disseminated a Bring Your Own Device (BYOD) policy?

Communication & Collaboration

1. Does your organization have audio and video conferencing capabilities for conducting virtual meetings?
2. Has your organization implemented a method of communication besides email? Examples: Teams for messages.
3. Does your organization have access to cloud-based IT infrastructure that allows remote access and file sharing?
4. Does your cloud license allow for easy scaling of computing resources?
5. Does your organization use project management software and are all remote workers trained for it?

Security

1. Has your organization created and disseminated a policy defining which cybersecurity tools remote workers are required to use?
2. Has your organization implemented email encryption and filtering software?
3. Do you require employees to use multi factor authentication to log in to your cloud platform?
4. For employees on mobile devices, do you have a Mobile Device Management (MDM) solution in place?
5. Do you require employees to enable automatic updates for their security programs and operating systems? Examples: antimalware apps, Microsoft Windows, Mac OSX.
6. Do you have clearly defined procedures for employees to escalate security issues?

Results Analysis

For each question answered with "No," carefully consider its relevance to your organization. Any of these has the potential to impact the security of your business and the productivity of your workforce. You may need to acquire additional equipment or software licenses, but the benefits will far outweigh the costs.

REMINDER: This self-assessment is designed to give you a **basic** overview of your readiness for implementing or expanding your remote work capabilities. To help you identify any unique requirements your organization may have, or address any of the "No" answers above, contact us today. Our expertise in creating and managing remote-work infrastructure will enable you to achieve high levels of productivity for your remote workforce.