Checklist: How to Reduce Security Risks for Your Remote Workers

Remote working can provide a significant advantage for your company and employees but there are risks. In order to ensure the security of your company, its data, and and that of your employees, you need to lay a solid foundation. This checklist helps you to improve security for all of your remote workers.

Cybersecurity

- □ Ensure laptops/devices have hardware encryption.
- □ Where possible, ask that screen filters are used to make shoulder-surfing harder.
- □ Make 2 factor authentication (2FA) mandatory for all remote workers, including email and when accessing any critical systems and applications.
- □ Encourage staff to use password managers.
- □ Ask staff NOT to defer critical updates to software.
- □ Remind staff that surfing explicit sites, amongst other things, is illegal.
- □ Staff must not visit sites like illegal movie websites as they pose a risk of ransomware and malware infection.
- □ Remind staff NOT to lend their machines to their children or other members of the family.
- □ Stress the IMPORTANCE of NOT sharing passwords (remote working can lead to more password sharing).

Privileged Users

Ensure you inform all IT & business privileged users and:

- □ Remind them of their responsibilities.
- □ Insist that they DO NOT log DAILY tasks with high privileges.
- □ Demand that they REPORT all errors/confess to mistakes immediately.

Phishing Emails

- □ Remind staff that it´s ok to make a mistake and that they should own up if they have:
  - □ Accidentally clicked on a suspicious file or link.
  - □ Opened a suspicious PDF or Word, excel file with macro.
- □ Identified a malware/ransomware infection and should report it immediately.

softwareONE

Checklist: How to Reduce Security Risks for Your Remote Workers

Online Meetings & Calls

- □ Remind staff to MUTE the microphone when they are not speaking in a conference call.
- □ Educate all staff to ensure webcams are blocked by default.
- □ Remind the staff NOT to leave their machines UNLOCKED, especially during a call or when taking a break.
- □ Ask staff NOT to work from coffee shops or public places (if possible) – especially if they are on confidential calls or working on confidential documents.

Expectations

- □ If you don't have one yet, create an exceptions register.
- □ Create a review by date and put multiple calendar reminders for you/your team to review them.
- □ Where possible, have a "No way this is an exception" list.

Cyber Attack & Incident Response

- □ Constantly remind staff to be alert for phishing emails and other attempts to compromise/steal account details.
- □ Staff must report these emails and malicious activity.
- □ Encourage staff to reach out to the IT team if necessary.
- □ Security staff must be extra vigilant and actively seek out suspicious activity (given the remote working habits of users this may be operationally expensive).
- □ Ask IT and security staff (including outsourcers) to pick up the phone and call if it's important rather than solely relying on email. Use a separate out-of-band app or something as simple (not very secure) as WhatsApp groups for urgent communications.
- □ Keep a printed copy of your procedures and checklists at home AND make sure they are not easily accessible.
- □ Remind all staff that it's ok to make mistakes (like sending emails to wrong recipients, clicking on a malicious link, causing an outage etc.) and that they MUST own up immediately. Stress that in most cases there will be NO repercussions

Privacy

- □ Remind all staff of their responsibility to respect the privacy of your clients and your staff.
- □ Staff must be reminded NOT to email personal information via email OR store personal information in non-approved locations.
- □ Remind IT and cybersecurity folks to be extra vigilant for possible malicious activities on user accounts.
- □ Staff members might exchange personal phone numbers or email addresses. Avoid this if possible, or add a note to delete the information after use.

Checklist: How to Reduce Security Risks for Your Remote Workers

Backup

□ Provide staff software to ensure their critical documents are backed up.

□ Ask staff to back up their data on an approved external hard disk that is NOT permanently connected to the device.

□ Ask staff NOT to use external cloud storage services.

□ Ask staff to reach out to discuss any cloud storage or cloud service solution that they want to use.

Source: Cyber Management Alliance, 2020

Keen to learn more?

If you're unsure of where to begin, consider the advice of our Security experts. When you partner with SoftwareONE, you'll know exactly where your risks are and how to protect your assets. We'll work with you to stay ahead of potential threats so you can tailor your work from home strategy to your specific business needs and better articulate to your team members what exactly needs to happen moving forward. Having said this we invite you to have a look at our additional Work from Home resources.

✓ Security Checklist for Remote Workers

✓ Monthly Cybersecurity Updates

✓ Future Workplace Content Hub

softwareONE

How can we help you?

Get in touch to find out more about how
to plan your Future Workplace!

SoftwareONE AG

Find us online at:
https://www.softwareone.com/en/topics/future-workplace

Disclaimer - The information provided in this advisory is provided "as is" without warranty of any kind. The use of this information is totally the responsibility of the user and SoftwareONE disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall SoftwareONE or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, claims arising out of negligence and/or misuse, loss of reputation, loss of business profits or special damages, even if SoftwareONE or its suppliers have been advised of the possibility of such damages.