Checklist: How To Secure Your Workplace When Working From Home

Securing Your Workplace

- [ ] Select a screen position so that neither family members nor strangers (e.g. the neighbor through the window front) can view information unhindered.
- [ ] Make sure your private Wi-Fi connection is secure. Most Wi-Fi connections are properly secured; however, older installations in particular can have weak points.
- [ ] Company devices (desktop, laptop and cell phone) should not be made accessible to children or other family members (NDAs also apply in the home office!).
- [ ] If necessary, use a privacy filter. (Also recommended for working on the go.)

Training Your Personal Behavior

- [ ] Activate the screen lock every time you leave your workplace.
- [ ] Do not send sensitive data unencrypted or unprotected via email.
- [ ] Do not send business information through private email accounts.
- [ ] Do not leave any information lying around in the home office, e.g. printed documents. Any data / information should be protected from family members.

Taking Phone Or Video Calls From Home

- [ ] Mute your microphone when not in use.
- [ ] Only take calls with a headset, headphones or smartphone - do not use the speaker built into your laptop.
- [ ] Deactivate your camera by default and keep it covered when possible. This not only conserves bandwidth,but also prevents sensitive information from being seen.
- [ ] Blur your background when in a video call to prevent the accidental disclosure of confidential information.
- [ ] Do not leave the workplace during an active telephone / video conference.
- [ ] Do not make any calls in public (balcony, open air etc.)
- [ ] Be careful with screen sharing. Pay attention to what content you share with other participants.

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