The Cyber Security Essentials Checklist for a Hybrid Workplace

What to keep in mind when establishing a cyber-secure hybrid work environment

☐ Make sure to have a hybrid work policy in place.	• The hybrid work policy should list all the software approved for use when working, ranging from email clients to approved cloud co-working spaces to instant messaging and file-sharing.
☐ Clarify your Bring Your Own Device (BYOD) policy.	• Are employees allowed to use their own devices? • Are there only specific programs allowed on personal devices? • Are employees aware of the best practices for protecting data on their devices, such as password/PIN access and screen locking?
☐ Establish a hybrid work clearance checklist. And follow through on it.	• What are the tools employees need to have to get clearance for hybrid work? • What knowledge do they need to have to be approved for hybrid work? • Have they read and acknowledged company security policies that are in place? • Phishing awareness
☐ Continue education and awareness training for all employees, with emphasis on:	• Raising awareness and understanding of insider risk • Confidentiality and data leaks • Ransomware attacks
☐ Guide employees through the fundamentals of network security.	• Ensure that all employees have access to and know how to use a company VPN. • Clarify that VPNs are not only for accessing company servers and data but also to ensure encryption happens on the go. • Make sure everyone understands that home WiFi is not necessarily as secure as one would wish. • Instruct employees to update their router firmware and update their WiFi SSID and password.
☐ Set clear guidelines for password management	• Mandate and enforce the use of password managers. • Require multi-factor authentication for work accounts. • Ensure that all devices, including phones and tablets, are password or PIN-protected and automatically lock after a period of inactivity. • Consider mandatory PIN protection for email clients on phones and tablets.
☐ Other best security practices	• When not in use, devices should be stored in secure locations where pets or children cannot access them. • Software should be updated regularly on all devices. • Only company-approved cloud services should be used

PhishNet