Remote Cybersecurity Checklist

KEY POINTS TO ENSURE CYBER HYGIENE IN REMOTE OFFICES

This list is a starting point that could help you evaluate security considerations for long-term remote work. The considerations listed here should be reviewed within the context of your organization's complete information security program with close attention focused on the specific threats, risks, and vulnerabilities unique to each organization.

1 Device Security

- [ ] Use company-issued devices whenever possible.
- [ ] If personal device must be used, dedicate it to company data access and do not share with other family members.
- [ ] Extend security monitoring and protection to all devices accessing company data and applications.
- [ ] Keep all devices updated with the latest operating system and application patches

2 Home Networking / Connectivity

- [ ] Verify that home WiFi routers/Apps are on the latest firmware and not using default passwords.
- [ ] Verify that WiFI encryption is set to enterprise level or to highest level allowed by the router.
- [ ] Avoid using mobile WiFi cards directly exposing PC/Laptop to the Internet. If mobile WiFi cards must be used, make sure windows firewall is on and configured to block all incoming traffic.
- [ ] Turn on firewall on WiFi routers and remove any port forwarding (if exists.)

Conisder Worry-Free Security With Endpoint Detection and Response

3 Connectivity to Company Data

- [ ] If VPN is used, disable split-tunneling to enforce company web security when connected to corporate network.
- [ ] Evaluate extending company web security solutions to devices at home even when not connected to corporate network directly.
- [ ] If Office365 is used, enroll all personal devices in Intune and establish conditional access policy.
- [ ] Establish logging and monitoring for printing to local home printers if allowed.

4 Communications / Collaboration

- [ ] Make sure conferencing/collaboration software is on the latest version and chats are secured
- [ ] Create only password-protected meetings
- [ ] Do not allow participants to join meetings before hosts
- [ ] Do not store recordings or sensitive data on videoconferencing provider's cloud

New York City | Boston | London | Luxembourg | Singapore
www.rfa.com | sales@rfa.com | US +1 212 867 4600 | UK +44 207 093 5010