Checklist for Working Remotely

Take essential actions to mitigate security risks –

1. **Turn on Multi-Factor Authentication Immediately.** Implement MFA to ensure no unauthorized party is remotely accessing the company's networks or user accounts Long passwords with multi-characters, and unique passwords for different systems and logins. The popular Microsoft Office 365 service includes MFA for free.

2. **Email Encryption / Best Practice** – Email is the most used digital technology and presents an open door for cyber-attacks. There are multiple solutions to secure email data.

3. **Ensure Security Features are Up-to-Date** – all devices should be protected with antivirus, web filtering, firewalls, device encryption and other preventative software.

4. **Discourage use of Public Wi-Fi** – Encourage the use of trusted networks when working with sensitive business data.

5. **Distribute Tech Support Contact Info.** Employees should readily have access to company IT policies, procedures, and contact information of critical IT personnel to whom security incidents can be reported and who can assist with technical issues.

6. **Avoid Storing Data Locally.** Employees should avoid saving data locally on their computers and instead utilize on company-approved network and cloud storage locations – the ones your company backs up regularly – as much as possible to store data.

7. **Don't Get Hooked** – Beware of Phishing Attacks. When employees receive emails or other electronic communication, they should be trained to identify potential phishing emails. Specifically, employees should be educated and reminded to
   - verify that the sender's email address matches the address of a known contact (especially on mobile devices, select the sender to see the real address);
   - hover over any link before clicking it to identify the destination;
   - be wary of emails that are unusually brief, unexpected, or out of character; and
   - refrain from opening suspicious attachments. If a seemingly normal email or communication is from an unverifiable or suspicious sender, then employees must be trained to report such phishing incidents to the company. Taking these precautions can reduce the effectiveness of phishing attacks.

8. **Share These Tips and Other Useful Insight.** Share this announcement and other resources discussing data privacy and security measures with all employees, team members, business partners, clients, customers, suppliers, vendors, etc. We are all in this together!

The ComputerLand Team is prepared to address your COVID-19 related or other data privacy and security questions and concerns. Please contact us today to discuss your current remote policy and do a security assessment of your current environment.

ComputerLand®
Silicon Valley
info@cland.com • (408) 519.3200 • www.cland.com