CHECKLIST FOR CYBER-SECURE REMOTE WORK

A comprehensive cybersecurity plan for teleworking should answer these questions:

- ❑ Has your IT/Security team approved all remote platforms and applications?
- ❑ Does your IT/Security team have visibility into all remote worker activities?
- ❑ Hacking incidents are up 400+% since Covid-19 crisis began; are you guarding against phishing and spear phishing threats?
- ❑ Are your employees trained in doing the basics to prevent breaches?
- ❑ Do you require strong password and username protections and two-factor authentication?
- ❑ Are you safeguarding sensitive information—are protocols in place, is sensitive data encrypted, have you eliminated license-sharing?
- ❑ Have you deployed a firewall?
- ❑ Have you mandated VPNs for remote use?
- ❑ Are employee WiFi connections secure and do employees understand that there should be no use of public WiFi connections?
- ❑ Do employees understand that work use should be kept separate from personal use for laptops, PCs, and smartphones?
- ❑ Can you encrypt where possible (Firevault works well for Apple products and Bitlocker for Microsoft products)
- ❑ Do you have a regular data backup system?
- ❑ Have you enacted a policy of limited/authorized only access? Access management is a key requirement for any cybersecurity policy.
- ❑ Do you communicate regularly with leadership on security threats and options?
- ❑ Do you have a resiliency plan for the next unexpected event?

For more information, visit icma.org/coronavirus.