Managing InfoSec Risk During a Global Pandemic
Key Takeaways – Recommendations for the Remote Workforce

1 1.Use company issued devices where possible

2 1.Be vigilant against phishing attacks, business email compromise, and COVID-19 stimulus fraud

3 1.Protect online accounts (use different passwords, clear browsing history, do not store passwords in browser)

4 Use a personal password manager (i.e. LastPass, KeePass)

5 1.Secure your home Wi-Fi network (WPA2/3, strong password, create guest network, disable UPnP)

6 Do not store company information on personal devices, email accounts, or cloud storage services

7 1.Use MFA (multi-factor authentication) for personal accounts, especially e-mail

8 1.Only browse on sites that use HTTPS and disable JavaScript

9 1.Turn on the home router firewall and the operating system firewall

10 1.Utilize an industry accepted anti-malware and anti-virus tool

11 1.Confirm that all your devices are updated to the latest software and firmware patch levels

12 1.Continuously back-up your data and confirm a copy is stored offline