RISKPOINT
INSURANCE ADVISORS

Convergence
NETWORKS

Cyber Security - Best Practices Checklist

□ **Update your Software:** Enable auto-updates for your all your Apps, Operating Systems and Web browsers. Remove old software you no longer require.

□ **Secure your Files:** Backup important files, have multiple copies and at least one that is offline (not internet accessible) and test recovery of your backups on a recurring basis.

□ **Encryption for Data at Rest:** Enable Device & Storage Media Encryption including on laptops, tablets, smartphones, data backup media, removable media & in cloud storage.

□ **Encryption for Data in Transit:** Enable WPA2 or WPA3 encryption for Wi-Fi. Use a VPN over public networks if available. Use HTTPS in your browser (not HTTP).

□ **Multifactor Authentication (MFA):** Enable this anywhere that it is available, especially for cloud-based apps and services.

□ **Credential Management:** Use a password vault with MFA to store your passwords and ensure you use unique passwords for your various accounts.

□ **Password Strength:** If you're using a password vault or password manager, there's no excuse for weak passwords. Make them strong & complex.

□ **EDR / MDR:** Use EDR or MDR in conjunction with Antivirus software.

RISKPOINT INSURANCE ADVISORS

Convergence NETWORKS

Cyber Security - Best Practices Checklist

□ **Least Privilege:** Tightly restrict use of administrative privileges and limit access permissions for everyday user accounts to the least amount required to achieve business objectives.

□ **Asset Management:** Keep an updated list of all your hardware and software including cloud-services that are in use in your organization.

□ **Get a Response Plan:** Establish a Security Incident Response Plan and practice it.

□ **Secure Remote Access:** If you use RDP, secure it by only allowing its use AFTER connecting via VPN. If you use a VPN, make sure you've got multifactor enabled for it.

□ **Email & Web Filtering:** Ensure your email service provider is using a secure email gateway to filter malicious email. Ensure you have a DNS or Web filtering service in place to block malicious web traffic and online threats.

□ **Email Authentication:** Enable DMARC on your email services to reduce risks of email spoofing. Get help if you don't know how.

□ **Vulnerability Scanning:** Establish a means to provide visibility over what software vulnerabilities exist across your devices.

□ **Cybersecurity Program**: Establish a cybersecurity program based on a well-known and established standard or framework. Get help if you don't know how.

□ **Cybersecurity Awareness Training:** Establish a means to provide regular recurring cybersecurity awareness training for your employees.

□ **Vendor Risk Management:** Develop a method for vetting the cybersecurity practices of your 3rd party vendors and business partners.