SECURITY CHECKLIST

The following is *not* a comprehensive list – Use for guidance based on industry standards, recommendations, and regulations.

1. **Keep Your Operating Systems Updated**
   Whether you run Microsoft Windows, Apple OS X or Linux, the operating system needs to be set for automatic updates. Consider turning off computers at night or rebooting promotes the installation of updates (and cleans system clutter). Updates are critical for Server Operating systems, since all patches and updates need be reviewed and updated on a recurring schedule. Employees need constant reminders to have their smartphones and tablets also set to update their operating systems automatically. Better yet, consider an EMM/MDM. Tools can be employed to automatically patch. Centralized patch management is best, so devices report to a centralized server that pushes known and tested patches to your devices and reports their status. You can also manually patch or fix non-compliant devices.

2. **Antivirus Updates**
   Ensure "check for updates" is enabled and that you scan your device frequently. Ensure any media that is inserted (Example: thumb and external hard drives) into a workstation is set to "scan before use." Devices should report the status of the antivirus updates to a centralized server, which pushes updates automatically when required (also known as "checking in").

3. **Strong Password Policy**
   IT policies should mandate complex passwords, meaning at least eight characters with a combination of upper and lowercase letters, numbers and special characters. In 2018, we generally recommend password lengths greater than 8 characters even if not a required minimum. Passwords should be changed every 90 days. If longer times are required, the password length should be increased. Most importantly, use a unique password for network access that you do not use elsewhere. If your Facebook account is compromised, you don't want your network account compromised. Never share your password. Tools can be employed to enforce a password strength policy.

4. **Use Automatic Screen Lock**
   When a workstation or mobile device has been idle for a few minutes, it should be set to automatically lock the screen to keep prying eyes out of the system. We recommend 10 minutes to meet most regulatory compliance requirements (15 minutes maximum, some regulations may require shorter times). Consider applying the same policy to webpage idle timeouts.

5. **Equipment Tracking**
   Know where your data resides, including servers, workstations, mobile devices, thumb drives, backup and replication systems and cloud locations. Limit access to only absolutely needed devices (least access security model). Use inventory tags and verify assigned devices to help track company-owned devices.

6. **Physically and Digitally Secure Devices**
   Any device that contains company and client data needs to be physically or digitally secured. On-premise file servers need to be in a locked room or equipment cage, and the office should have a security system. Mobile devices need to be locked when not in use. Data drives should be encrypted.

7. **Dispose of Data/Equipment Properly**
   All unnecessary physical files and draft documents with personally identifiable information should be secured and shredded to minimize risk. Workstations and other mobile equipment used for processing data should be device wiped (Ex: DOD wipe is 7 passes of 0s and 1s). Otherwise, physically destroy the hard drive to minimize risk of data recovery.

8. **Encrypt Backup Data**
   The company should encrypt any backup media that leaves the office. Strongly consider data encryption at rest. Validate that the backup is complete, and test restores (validate backup). The company should regularly review backup logs for completion and restore files randomly to ensure files will work when needed. Test backups with frequency.

9. **Minimize Administrator Privilege Use**
   Allowing workstations to run with local administrator credentials exposes systems to many security threats and can lead to an entire network infection. Do not work regularly on a workstation with Administrator access. General/daily use accounts should not be Administrator accounts. Admin accounts should be separate. Tools can be employed to ensure role assignment changes result in rescinding access.

10. **Send Secure**
    Use tools that allow for the secure sending and receiving of secure files. Enforce tools that automatically scan for sensitive data. All personnel should be educated on using the portal or encrypted email solution for any file containing confidential data. Include methods such as # or [ ] in subjects to simplify use. Use automatic encryption whenever possible, but train users to understand this is not a given.

11. **Connect Securely**
    Use a secure remote access by either utilizing a VPN (virtual private network) or other secure connection (look for the https: in the web address bar), such as Horizon View. Employees should only connect to public Wifi for work if they are sure it's authentic and trust the source (by verifying the SSID/password with the client). If you are unsure about the Wifi quality, use a 4G LTE mobile hot spot, or connect through hotspot capability on your smartphone. Users should ALWAYS use encrypted transport when connecting remotely.

12. **Protect Mobile Devices**
    Mandatory passwords and encryption should be extended to smartphones and tablets. You should have a process to notify IT personnel if a device is misplaced or stolen and a tested process to erase the mobile device of all company data remotely. Best case, use an EMM/MDM that provides containerization of corporate data so an enterprise wipe can be performed to only wipe company info from the device, not the entire device.

13. **Update IT Policies**
    Review IT/computer usage policies and provide annual (or quarterly) training to employees for all new and updated policies. The company should include adding wording on BYOD (Bring Your Own Device), Remote Access, Privacy (and acceptable use) and Encryption where appropriate.

14. **Awareness Training**
    Employees need to be reminded to be suspicious of emails that are out of character. Employees need to be shown how to hover over an email link before clicking and to look at email properties to see if the sender's email address matches. Remind employees to not forward suspicious emails to anyone else and to contact IT for assistance. Forwarding email is not ideal, and now someone else may inadvertently click the link because they trust the person forwarding the email and are not validating the initial sender. Consider using a phishing tool monthly that will test your users. Then provide additional training for those who require it. Vishing is a common threat similar to Phishing that occurs over phone calls. Awareness should include phone calls, text messages, packages (especially with free content), and other methods of communication and how to get help and escalate.

15. **Educate Employees**
    Security education is as important as professional education and should be required frequently and routinely. Security is a lifestyle and a perishable skill – so the best recommendation is monthly. In addition to reviewing policies, employees should be educated on current cyber security attack methods, such as phishing, account take overs and threats, including Ransomware and social engineering used by hackers to access a user's computer (i.e. NEVER provide your login, password or confidential information over the phone or to people you don't know). Ensure your company policy tells employees to not share their password with anyone, including internal or contracted IT staff.

16. **Vulnerability Scanning**
    Conduct regular vulnerability scans on all devices. This will identify patch management weaknesses and areas that are susceptible to known attacks. Follow policies, but expedite patching of these systems. Consider patching based on severity of the vulnerability; critical vulnerabilities should be patched within 3 days, high 1 week, medium 1 month, and low within 1 quarter. Time frames are subjective! Not all vulnerabilities are resolved with a patch. Many require a reconfiguration or other system changes.

17. **Background Check Potential Employees and Contractors**
    Complete a thorough background check on all potential employees or contractors before allowing them access to your data or systems. With today's Internet connectivity and tiny USB storage devices, thousands of files can be covertly copied in minutes, without anyone else realizing it. All a bad actor needs is for the company to grant access.

18. **Require Facility Escorts and Visitor Badges**
    Prevent employee tailgating! Employees should be reminded to challenge anyone that is in the office that they don't recognize ("Hi, can I help you?") and provide them assistance to find the company employee with whom they are meeting. If the visitor appears suspicious, the employee should notify someone from management or administration immediately. The key point is you need to have a policy and train your employees. It is best to require visitors to sign in, provide some sort of authority-issued ID and then give them a clearly visible guest badge.

19. **Outsource Security**
    Hire experts when implementing firewalls and security-related features, such as remote access and wireless network equipment so that it is properly configured the first time. Chances are your internal IT

staff has not been exposed to optimum security training, or they don't have experience with setting up a new device. Consider external resources to perform penetration testing to identify and lock down any system vulnerabilities.

20. **Have an Incident Response Plan**
    Companies should have a security incident response plan if there is concern that company data has been compromised. This would be in a written format and include information on educating personnel on how to document the events leading up to the breach discovery, notify appropriate company/external IT personnel of the breach so they can take steps to stop it and develop an internal and external communications plan. Be aware that incident response is often not provided by managed service providers. You may be required to use specific companies by your cybersecurity insurance provider.

21. **Cybersecurity Insurance**
    Unfortunately, you can complete the checklist items above and still fall victim to a hacker. To protect against that possibility, you should consider cybersecurity insurance. The cost of this insurance has come down considerably in the last decade. Companies should evaluate both first-party insurance to cover direct losses resulting from the breach (downtime, recreation of data, direct remediation costs) and third-party insurance to cover any damages to clients whose data may have been compromised.