CHECKLIST: EMPLOYEE OWNED DEVICES

While we hope and pray the Coronavirus will not affect you and your business or any of your employees or community, recent events compel us to offer the following advice should you need to implement a work from home plan. Cybersecurity is already a big enough concern. If you send employees to work from home and don't have a good game plan, you could be opening your business up to some big risks or threats making cybersecurity a much bigger concern.

Our goal with any of our clients is to help them have a solid strategy when it comes to implementing technology. This will allow our clients to have a functional system, productive employees and the risks have been considered and addressed.

If you're not one of our customers and you need some guidance, this checklist is meant to serve as "things you should consider" when sending your employees to work from home to allow for a functional system, productive employees and to mitigate security risks. These are all Yes/No questions. All questions are designed so that if the answer is Yes, then it is a positive or good thing. Depending on how your business network is setup, some of the questions may not apply to you. You should be especially concerned about employee owned devices (laptops or desktops, etc.) entering your network because they could have existing problems that may compromise your network, which is what this list is for.

Everyone's situation is different, this list is not intended to be a comprehensive checklist to cover every situation. We are available to discuss a plan to guide your organization, or you can use this information to do your best on your own or with your Technology Partner to making working from home a reality if needed.

EMPLOYEE OWNED DEVICE CHECKLIST:

1. **Question:** Has the employee received security awareness training? ☐Yes ☐No
    a. **Explanation:** Security Awareness Training is the process of training employees on how to properly use computers to increase their ability to make good decisions and reduce the risk of a hacker gaining access to the device.
    b. **Why we are asking:** Employees are often the weak link when it comes to security, an employee that makes poor decisions when using the computer can become the door for hackers to get access to your data.
    - **Recommendation:** Enroll employees in security awareness training. On of our partners, KnowBe4 is providing free online security awareness training in response to COVID-19. To access the free training go to https://www.knowbe4.com/homecourse - the password needed to access the content is "homecourse"

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209

CHECKLIST: EMPLOYEE OWNED DEVICES

2. **Question:** Is a host-based firewall turned on? ☐Yes ☐No
    a. **Explanation:** This is the firewall on the actual computer – not a firewall appliance in the home. For example, Microsoft Windows and Apple OSX (two most popular operating systems) both include a firewall that is built into the operating system.
    b. **Why are we asking:** Ensuring this is on will add an extra layer of protection from devices connected to the employee's home network, particularly if those devices have been infected by a virus or some other form of malware.
    c. **Recommendation:** Turn on host-based firewall

3. **Question:** Is the computer dedicated to employee? ☐Yes ☐No
    a. **Explanation:** Many devices in the home are shared with the other members of the home, such as a spouse or children.
    b. **Why we are asking:** Family members may not have received security awareness training and practice poor internet hygiene resulting in computers laden with malware and viruses. Connecting these computers to company resources no matter how it is done poses a business risk.
    c. **Recommendation:** Ask the employee to dedicate a computer to business purposes where feasible

4. **Question:** Is there a strong password or passphrase on the computer? ☐Yes ☐No
    a. **Explanation:** A strong password is a minimum of 8 characters with numbers, symbols, uppercase and lowercase letters. A strong passphrase is something long but memorable, such as "My dog Jack knows 10 tricks!". The longer the length of the passphrase, the more difficult it is to crack.
    b. **Why we are asking:** Employee owned devices with access to company resources need a strong password on the computer to ensure someone that is not authorized does not gain access to the computer.
    c. **Recommendation:** Set a strong password, or passphrase on the computer.

5. **Question:** Is Anti-Virus software installed and up to date? ☐Yes ☐No
    a. **Explanation:** Up to date Anti-Virus software is critical to a device's security.
    b. **Why we are asking:** Having current Anti-Virus software can prevent processes and applications from running malicious code and protect your device and company resources.
    c. **Recommendation:** Install a quality Anti-Virus program and ensure that it is up to date. Our current recommendation for employee owned devices is Sophos Home Premium found here: https://home.sophos.com/en-us.aspx.

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209

CHECKLIST: EMPLOYEE OWNED DEVICES

6. **Question:** Is the employees home wireless network using WPA2 + AES? ☐Yes ☐No
    a. **Explanation:** Wireless routers have a variety of options available to encrypt the wireless communication, WPA + AES is currently the standard to ensure data on the wireless network is protected. Someone can take advantage of weak Wireless encryption is when they are in proximity to your wireless network.
    b. **Why we are asking:** To protect business data you want to ensure that all communication is done over an encrypted connection. Even if the employee is connecting with an ethernet cable, weak algorithms and password can put your business at un-necessary risk.
    c. **Recommendation:** Change the Wireless Encryption algorithm to WPA2 + AES

7. **Question:** Is the employees home wireless network using a strong password? ☐Yes ☐No
    a. **Explanation:** Wireless passwords (PSK's) under 20 characters in length have relatively low levels of security and can be subject to a dictionary or rainbow attacks.
    b. **Why we are asking:** Many consumers fail to change the default password, or they set a weak password on the wireless router. This can expose their wireless network to a local hacker that is trying to access their network.
    c. **Recommendation:** Change the password to something 20 characters or more.

8. **Question:** The operating system is at least Windows 8, or Apple OSX High Sierra? ☐Yes ☐No
    a. **Explanation:** The operating system is the software that is required to run the computer, Windows 8 and Apple OSX High Sierra or the last supported operating system from either manufacturer.
    b. **Why we are asking:** Software makers, such as Apple and Microsoft will only continue to provide security updates to supported operating systems. Running unsupported operating systems that do not receive regular security updates poses a significant cyber security risk to the computer and your business.
    c. **Recommendation:** Only use operating systems that are supported. This would include Windows 8, Windows 8.1, Windows 10 from Microsoft and macOS High Sierra 10.13.6, macOS Mojave 10.14.6, macOS Catalina 10.15.3 from Apple.

CHECKLIST: EMPLOYEE OWNED DEVICES

9. **Question:** Are applications patched and automatic updates turned on? ☐Yes ☐No
    a. **Explanation:** All applications and operating systems have vulnerabilities that need to be updated on a routine basis.
    b. **Why we are asking:** Vulnerabilities are one of the largest attack vectors for cyber-criminals, unpatched operating systems and applications leaves your computer exposed and an easy target for hackers.
    c. **Recommendation:** Turn on automatic updates for either Apple OSX or Microsoft Windows. Remove unneeded 3rd party applications to limit the number of applications that can be vulnerable to attack. Ensure all programs that are retained on the computer are updated to their latest version. Common 3rd party products such as Adobe Flash, Adobe Reader, Google Chrome, Mozilla Firefox, Mozilla Thunderbird, and Java are often exploited.

10. **Question:** Is the drive on the computer encrypted? ☐Yes ☐No
    d. **Explanation:** Drive encryption with Microsoft BitLocker (requires Windows 8 Pro or greater) or Apple Filevault makes the hard drive unreadable to those without the required password.
    e. **Why we are asking:** Encrypting the hard drive can prevent sensitive data from being accessed if the workstation or hard drive is stolen.
    f. **Recommendation:** If there is confidential information on the drive, particularly if you need to meet compliance requirements such as HIPAA, encrypt the drive.

About AZCOMP Technologies

Locally owned, AZCOMP Technologies has been providing IT solutions to small businesses since 2000. Our specialty is medical and dental practices, but we help a wide variety of small businesses by providing IT solutions, support, security, and strategy. Companies in Arizona benefit from our unique ability to consistently deliver phenomenal technology results, which includes dependable technology solutions, productive employees, minimized risk and strategic planning. Are you working with someone that can deliver such value?

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209