More likely than not, most employers are seeing some form of remote working arrangements whether it is typical remote employees or those that are now working remotely due to current circumstances. There are certain steps companies and their employees should take to protect personal information and other confidential data.

Below are our top ten tips for people working remotely. This list should start the process, and as the circumstances allow or require, companies should build in even more protections.

1. **Confidential Data Awareness**
   Remind employees about confidential data, including both personal data and business data, such as trade secrets. Make sure documents are not downloaded unless necessary and minimize transmission. If confidential data must be emailed or shared, use encryption.

2. **Proper Tools**
   Make sure employees who do not typically work from home have the right equipment and know how to use it. This includes privacy and security tools, such as VPN, remote meeting technology, secure electronic and physical document storage, including shredders if necessary.

3. **Equipment Protection**
   Some people may try to make sure their equipment is sanitized – which may cause more damage than it prevents. Educate employees how to clean equipment to avoid incorrect uses of sanitizers on electronics.

4. **Anti-malware and Patches**
   Remind all employees that virus detectors and patches need to be up-to-date. Make sure there are not competing services on the same device as one may impact the effectiveness of another.

5. **Passwords and Multi-factor Authentication**
   Protecting access into systems and tools is critical. Change the default password on home equipment such as routers. Password manager tools are effective in assisting to keep passwords secure, using complex passwords, and avoiding the use of the same passwords across accounts. Check with your security team about approved services, such as LastPass. In addition, multifactor authentication is one of the best tools for keeping accounts safe. If you have not implemented this, consider it.

6. **No Document Printing**
   A home environment is not the best for paperwork. Restrict printing unless absolutely necessary. Where it is necessary, require shredders or offer a shred-at-work solution using a dedicated shred box at home.

7. **Document Sharing and Storing**
   In order to assist with no document printing, develop or enforce a document sharing protocol. Restrict or permit as necessary cloud storage tools, such as Dropbox, Box, Google drive, OneDrive, etc. People will tend to retain everything and it may not be needed. Encourage minimum document retention and advise employees to check temporary storage and downloads.

8. **Work Devices**
   Work devices, including phone and laptops, should not be shared with other people. Especially now, there are likely other people in the house who may require distractions.

9. **Personal Devices**
   Not everyone has a work device available and may be working on a personal device. If so, develop a checklist for what should be in place on devices. Anti-malware, encryption, password managers and VPN are some basic tools.

10. **Cleansing Data**
    Be prepared to have employees clear the data on their devices and stored in the cloud on a regular basis, such as weekly. In all cases, have a plan for clearing data once standard work hours resume.

Last, if you have questions, please reach out to your manager or your IT / security department. If you have doubts about doing something with personal or confidential data, set yourself and your company up for success and ask the questions.