The New Normal – Technology Needs/Considerations

Employee Input

IT had the opportunity to review feedback from several departments regarding technology needs for a long-term teleworking scenario. A summary of those needs is detailed below.

Connect to the Network

Several employees would just like the ability to connect to the network in order to do their work as opposed to having to work solely in OneDrive or SharePoint. This can be accomplished via a laptop or a Remote Desktop Connection, depending on the individual's needs.

> *Laptops* – Laptop costs range drastically depending on availability. Recent purchases have laptop costs ranging from $1,000 - $2,100.
>
> *Remote Desktop Connection* – Employees can connect to their desktops from their personal devices, if their devices meet some basic requirements. License cost for this is $94.

Monitors

> The #1 request from employees was another monitor. Laptop screens are small; in addition, many employees are used to being able to drag windows from one monitor to another.
>
> The preferred way to address this is for employees to use spare personal monitors or TVs to act as 2nd monitors to their laptops, if possible. IT can provide connectors/cables to help out with this.
>
> If personal monitors or TVs are not available:

- If employees are utilizing County issued laptops, employees could bring monitors home. This would require IT to asset tag monitors which are leaving the building, employees to pick up and transport monitors (which are easily breakable) and then to have IT Help Desk staff work with employees on connecting their monitors.
- If employees are utilizing their personal PCs to connect to the County network, the employee would need to research the capabilities of their personal device to determine if it could support a 2nd monitor.

Printers

> Several employees requested printers.
>
> Because employees can't currently print, we've learned that they are emailing work related items to their personal email accounts and then printing those items on their home printers. This is a potential security risk for the County. Once an employee has emailed him/herself a document, that document has left the County network and all of our security controls. In general, **employees should not email County data to their personal email accounts**.

When employees email PII and other sensitive data to their personal email accounts OR when employees print PII and other sensitive data to their personal printers, it presents a **serious security risk for the County**. Email servers and networked personal printers can be breached; personal printers with embedded storage devices can be stolen, lost or disposed of without the device being cleaned.

We need to keep PII, sensitive and confidential data on County networks, devices, and cloud services approved for the storage of PII. If we've followed the news over the last several years, we know how devasting comprised PII can be for the impacted individual. **This is something that we should all take very seriously.**

As we become a teleworking society, our printing needs must change. Processes will need to be streamlined and the need for wet signatures eliminated. However we aren't there yet so, for the time being, we need to address the immediate need utilizing the following methodology.

Why does an employee need to print? Is it for convenience only… to proof read, to double check work, or is it just easier for them to comprehend and see on paper?

- Explore a second monitor. Being able to drag a window from one monitor to another provides an employee with the opportunity to continue working on one screen while reading and seeing the information on another.
- Set up a schedule for employees to come into the office to use County printers.
- Talk with IT to determine if there are other printing options available for your unique set up.

An employee prints because a wet signature is required. Let IT evaluate that situation. We are implementing Adobe Sign throughout the County to eliminate the need for wet signatures when possible.

An employee prints because they need to produce a form for an outside agency that only accepts a wet signature or a paper copy.

- If an employee must print, determine if they are printing PII, sensitive or confidential data.
- Printing PII, sensitive or confidential data? The employee should be issued a County approved printer and educated on the proper way to secure physical documents.
- Not printing PII, sensitive or confidential data? Talk with IT to determine if there are other printing options available for your unique set up.

- **Why is IT not in support of County issued printers in employees' homes?** Printers are one of the most difficult items to maintain; they are mechanical devices composed of a bunch of moving parts, many made out of plastic. Unlike most IT equipment, they cannot be maintained remotely; they require hands-on maintenance. They break, they jam, they don't feed properly, they don't print properly, etc. They present a unique maintenance challenge. Putting printers in employees' homes will put a strain on the IT Help Desk and leave many employees frustrated.

Better internet connectivity

Some employees do not have internet connectivity or have spotty internet connectivity.

Wireless hotspot - We have provided some employees with wireless hotspots (MiFis). Wireless hotspots use wireless mobile phone networks to provide an internet connection for employees.

- Purchase price ranges depending on availability - $0-$50; monthly cost $40

Raven modems – When we weren't able to get MiFis, we provided some employees with Raven modems as a stop-gap solution. Raven modems are designed for industrial applications. When we received MiFis and had to retrieve the Raven modems, some employees complained that the MiFi did not perform as well as the Raven modem.

- Purchase price $500; monthly cost $40

County issued phones

Employees do not like forwarding their desk phones to their personal cell phones and would like county issued phones.

County issued smartphones – the phone device is free; the monthly cost is $50

County issued flip phone – the phone device is free; the monthly cost is $30

Softphone - A softphone is an option for employees who have County issued laptops. A soft phone is basically your desk phone but it is on your laptop; it looks and works the same way as your desk phone.

The cost of a soft phone license is $200. However, for those employees who are permanently teleworking, we could transfer their phone license from their desk phone to a softphone. When the license is transferred to the softphone, the desk phone will no longer work. If a permanently teleworking employee needs to come into the office, they would need to bring in their County issued laptop in order to have a phone. It is not manageable to transfer licenses back and forth between desk and soft phones on a daily basis.

Unique Needs

A few employees have specialized equipment (desktops, printers, monitors, etc.) because of their specific job responsibilities. Recreating an employees' office environment in their home, although not impossible, is difficult to set up and support. IT would recommend that, if possible, these employees be provided County offices so that they can safely work on their equipment in the County building.

Software applications

Due to teleworking, new processes and procedures are being developed throughout County government. As a result, IT is being asked on a regular basis, to quickly evaluate and implement new software applications. We are completely on board with this and excited to work with our user community on the acquisition of new and enhanced tools. However, we caution that software does not always work as advertised and that software is *never* implemented as quickly and as smoothly as technology salespeople lead us to believe. Even though our needs are rapidly changing and evolving, we still need to evaluate software acquisitions for functionality, security, compatibility, duplication and cost.

Additional Considerations

Security

As we grant an increasing amount of remote access to County information assets for the purposes of telework, the risk of credential theft and loss increases. The best tool to help mitigate this risk is the purchase and implementation of a multi factor authentication (MFA) for our externally facing authentication interfaces. MFA reduces the risk of credential theft by requiring one or more additional factors of authentication to the one factor we currently have in place, passwords. A factor is something you know (password), something you have (hard token or mobile device), or something you are (biometrics). An attacker would have to comprise all required authentication factors to compromise our remotely accessible information assets.

Desktops vs laptops

To address a future of teleworkers and to be able to quickly react to a national emergency, we should eliminate desktops and provide employees with laptops and docking stations. This is an expensive goal but one that we should shoot for.

Summary

- Many technology issues mentioned by employees can be easily solved with the purchase of licenses and equipment.
- Employees must be educated on what data is considered PII, sensitive or confidential, understand the controls required to handle and protect and agree to abide by those controls.
- We need to identify if printing is absolutely necessary and, if not, help our employees to find other ways to address their printing needs.
- The more equipment we put in employees' homes, the more strain on the IT Help Desk. Troubleshooting an issue in someone's home is more difficult and time consuming than troubleshooting an issue down the hall. Additional Help Desk staff may be required or temporary part time employees.
- While teleworking, we must continue to remain focused on IT security education and controls. To bolster security, we should implement multi-factor authentication.
- We should eventually replace all desktops with laptops and docking stations.

Guidelines for the Safe Handling of Personally Identifiable Information

Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information. Each category of information used by the County requires a case-by-case assessment of the specific risk that an individual can be identified. Be aware that non-PII can become PII whenever new information is made available and can be linked to the preexisting information to identify an individual.

PII is an especially sensitive class of information as its misuse, loss, or theft can lead to disastrous consequences for the County and its employees, contractors, and residents.

General guidelines to follow for the protection of the County's PII assets include:

- Do not collect or accept PII from sources outside of Charles County Government unless it is required for a specific business use purpose.
- Do not share PII with others unless the entity you are sharing it with is authorized to access the PII and the sharing is required for a specific business use purpose.
- The County's PII should never be used for a personal business reason.
- The County's PII must be stored in locations which have the proper controls in place to restrict access to it and mitigate its loss. These locations include Charles County Government file servers and Cloud Services Providers which have been approved by the County for the storage of PII.
- Devices used to access the County's PII must be owned, managed, and secured by the County and should have storage encryption, anti-malware, and firewall software enabled and running.
- Do not allow others to view your device's screen or monitor when accessing PII unless they are authorized to access the PII.
- Remember to lock your devices before walking away. Windows devices can be locked by pressing the Windows key and the "L" key at the same time.
- Mobile devices should be physically secured against loss or theft when not use.
- The storage, processing, and printing of the County's PII is prohibited on personally owned devices.
- The transfer of the County's PII to personal email or other personal cloud services is prohibited.
- Encryption must be used when transferring PII to an authorized individual or entity.
    - Secure methods of transferring PII include encrypted email via Outlook Message Encryption and the County's OneDrive or Sharepoint sites.
    - Care must be taken when transferring PII to ensure that it is transferred to the correct destination and access is only allowed by the intended recipient.
- External storage devices used to temporarily store PII must be securely encrypted. BitLocker To Go with a strong password is a supported tool which can be used securely encrypt external storage devices such as flash drives.
- PII in paper form must:
    - Be secured in a physically locked location out of sight when not in use.
    - Never be placed in the view of persons not authorized to access the PII.

    - Be securely destroyed when no longer needed in paper form. The use of a cross-cut shredder is an easy way to securely destroy papers containing PII.
- The use and protection of some types of PII, such as Protected Health Information or credit card holder data, is regulated by law or industry standards. Authorized users of Charles County Government's technology assets must follow all applicable laws and regulations concerning the use and protection of all PII to which they have access.
- Immediately report any unauthorized access, loss, or theft of the County's PII to your supervisor and the IT Help Desk. The IT Help Desk can be contacted via email at ithelpdesk@charlescountymd.gov or via phone at 301-645-0614 (ext. 4357)

Cleaning technology equipment

General cleaning guidelines:

- Do not get electronic equipment wet; at most use a lightly dampened cloth
- Be sure to thoroughly dry any device after cleaning
- Do not use liquid or spray cleaning products directly on any technology equipment; do not bring liquid cleaning products near any technology equipment

Keyboards, mice, desktop computer buttons, desk phones, docking stations, printers/scanners hard surfaces of headsets, and any other hard-surfaced technology equipment:

- Wipe down these surfaces with alcohol-based wipes and dry thoroughly
- If you do not have alcohol-based wipes, spray a clean cloth with a disinfectant spray containing at least 70% alcohol and wipe the item, and then dry thoroughly

Desktop monitor screens and laptop screens:

- The proper cleaning procedure varies from screen type to screen type, and manufacturer to manufacturer.
- Never use liquid or spray cleaning products, or any disinfectant wipes, on a monitor or laptop screen. Active ingredients in these products may damage the screen and any anti-glare film.
- In general, to clean a screen, turn the monitor/screen off. Use a microfiber cloth to GENTLY wipe the screen down. If necessary, lightly dampen the cloth with water. Do not push hard on the screen. Follow up again with a dry microfiber cloth to remove any streaks.
    - This method simply cleans the screen but does not disinfect it.
- IT is looking into the purchase of cleanable screen protectors