IT Checklist for Employee & Equipment Return to Employer Facilities in 2020

☐ Returning Device Security

- **Rogue devices connecting to company network** – communicate what is acceptable and what cannot be connected directly or via Wi-Fi.
- **Home Laptops** – communicate what is acceptable and what cannot be connected to your networks without prior authorization. Ensure required Anti-Virus is installed if BYOD is allowed. Require consent to scan for malware if so. It may be as simple as forbidding work on personal laptops and devices in a company facility without prior approval.
- **USB/Flash/Thumb Drives & Network Storage Devices** – Personal storage devices should be prohibited. You should clearly communicate that they will not be allowed to connect to company computers and networks. If not already prepared, you should enforce device control to block unauthorized USBs and other unapproved peripheral devices.

☐ Asset Inventory & Future Needs

- **Return of all company equipment** - Everything that you are expecting back upon their full return to the office. If you are doing this in phases or shifts, plan the return communication accordingly. Reassess your deployment strategy, offloading, and future obsolescence.
- **Plan accordingly for employees that may stagger workdays between home and office while in transition.** You will want to make sure that they are fully productive and not needing time for unnecessary installation each morning they shift locations. Workstations that are properly sanitized after each workday can be shared to allow employees to have proper equipment at both locations.
- **Update inventory now.** If you have not done so, ensure managerial reporting and employee self-reporting are completed prior to return so you have an up-to-date inventory of this equipment, current location, and name of employee in possession.
- **Communicate**. Communicate that all employees must return company equipment that was deployed for remote work upon their full return to working from the office. This includes all screens, cables, and accessories.
- **Discuss compliance issues with HR.** Make sure that directives and requirements are legal and implemented correctly. If you plan to shift to a more remote workforce, discuss compliance and legal issues with Human Resources to eliminate any inequity claim by an employee or group of employees. They will guide you on discretionary decision limits regarding individuals versus departments or work type.
- **Discuss business class solutions for any former office employees that will now work remotely.** While temporary solutions may have been sufficient for this period, if you have decided to allow former office employees now to work from home instead, you must assess if stronger security is a wise investment. We highly recommend that you consider business class Wi-Fi (remember those conference calls with people dropping voice, video, or all together), Anti-Virus, VPN access, a Firewall, etc. to ensure that you are not infiltrated from any device in the home including IoT devices.

☐ Software License Inventory

- **Audit all Software Licenses**. Do this especially for employees that required certain licenses that are not longer needed. For example, many companies added licenses for video conferencing software that was well utilized during this instance can be cancelled upon return to the office to reduce expenses.
- **Estimate Cloud Resource Usage Decline**. You may have expanded cloud usage greatly during this time, but this may no longer be necessary. This is another place where an audit and decision to decrease can save expenses.

☐ Update Operating Systems and Software

- **Ensure that all employees have not ignored updates or rescheduled indefinitely.**
- **Update computers and servers that were left on premises**. Especially check those that were shut down during this period.
- **Update Patches.** Along with updates, ensure all patching on all devices is done as soon as practically possible.

☐ Unregistered Software

- **Get rid of it.** Some employees may have downloaded software that is not registered with your organization. Whether this was done unknowingly, in an effort to save time, or to get around seeking IT approval; identifying and eliminating any unregistered software on company devices must be mitigated as soon as possible. Your detection solution should inventory software and report on application risk levels

☐ Security Scanning, Remote Monitoring & Maintenance (RMM), and Endpoint Detection & Response (EDR)

- **Ensure all protections are enabled.** All devices used at home should have been secured during this time, but you may instance where an employee disabled software in order to perform certain actions. Communicate with employees that they must report if this happened, but since some may not, you must ensure that all protections are up to date.
- **Employ Updated Vulnerability Scanning, RMM, EDR to ensure that all endpoints are secure.**