IT, REMOTE WORK AND CYBERSECURITY CHECKLIST

A working checklist of steps to take to transition to remote work and enhance cybersecurity during COVID-19 and similar crises.

Transitioning to Remote Working

- o Create an outline for expectations for remote work, including daily check-ins, timekeeping, flexible work schedules, internet connectivity requirements, and equipment requirements. (Samples of these can be found in MAPP's Working from Home Policies Benchmarking Report)
- o Generate a list of departments and individuals allowed to work from home and who approves the ability to work remotely.
- o If applicable, create an equipment "check-out" form for employees who need to take home laptops, tablets, phones, or other materials for their remote work.
- o Decide on a virtual meeting medium, such as GotoMeeting, Zoom, or JoinMe, and include links to training for all remote employees.
- o Decide on an instant messaging software, such as Teams, Slack or Google Hangouts, to allow teammates to quickly connect without cluttering email. Provide links to download instructions and training to employees.
- o Generate work from home etiquette for the teams which outlines proper communication channels, online work etiquette, and standard expectations for sharing information.
- o Ensure a secure VPN for all workstations.
- o Ensure all critical software programs and access are available for remote workstations and install before moving remote
- o Confirm all software updates and security/firewall has been updated on all remote workstations.
- o Communicate with critical suppliers and customers that teams will be working remote and discuss any potential challenges or changes that may occur.
- o Provide employees remotely with a "remote working" out-of-office email reply so senders know that responses may be delayed or triaged based on the current situation

Best Practices

- o Have the CEO post a message each morning to set the tone for day, including any updates on business, the economy, customers, challenges and gratitude. These are even more powerful if it is on video so viewers can connect on a deeper level with the message.
- o Schedule daily or weekly "huddles" on a virtual meeting platform where employees can talk about challenges, productivity issues, and socialize to maintain communication, connectivity and culture.
- o Send daily or weekly newsletters to drive a positive online/remote culture. These could include upbeat music videos, motivational quotes, photos of pets and children, and other celebrations.
- o Share resources on topics that include personal wellness, best practices in working from home, dealing with anxiety, and unwinding/disconnecting after a challenging day.
- o Continue to provide information about any employee assistance programs or resources to help with counseling, legal or financial support.

Notes:

IT, REMOTE WORK AND CYBERSECURITY CHECKLIST

A working checklist of steps to take to transition to remote work and enhance cybersecurity during COVID-19 and similar crises.

Remote Work and Cybersecurity

- o Remind all employees to be hypervigilant during this time. Cyber crimes tend to increase during an emergency or crisis. Employees should delete any unsolicited emails from unknown senders and never open attachments in unsolicited emails regarding COVID-19.
- o Remind your staff of security procedures, protocols.
- o Offer additional staff training with regular reminders and tests to ensure all remote workers have an understanding of good cybersecurity practices.
- o Ask your IT team or company about mobile device management for laptops and other mobile devices so you can remotely manage and wipe a device if necessary.
- o Develop or update your data back-up strategy. All files should be backed up regularly, so in case of a cyber attack (such as ransomware) not all is lost.
- o Ensure that all employees Wi-Fi connection is secure, and ask to not use a public wi-fi connection if possible.
- o Setup firewall and antivirus on all remote workstations, and make sure they stay up-to-date.
- o For any and every critical business transaction, ensure that mulifactor authentication is in place.
- o Develop and share a strategy with all workers on protocols in case of a cybersecurity breach.
- o Work with your IT team or IT company to set up plan for monitoring access to company documents, workstations and data.
- o Review and update all IT projects and re-prioritize with an understanding of the current crisis and potential challenges with remote workstations and cybersecurity.
- o Remind employees to keep their work and personal accounts separate, and not use personal email or cloud-storage for company-related business.
- o Offer an easy and efficient way for employees to report any IT issues or suspicious activity to your IT team or company.

Notes: