FULLSCOPE IT

Excellence in Remote Working Checklist

how to keep your team afloat in a global pandemic

Remote Collaboration Platforms

- ☐ Consult with trusted advisors to make good decisions regarding remote working – executive leadership, IT and business units
- ☐ Ensure that you don't already have existing licensing for remote collaboration not being utilized
- ☐ Decide on a company authorized toolset - there are a variety of great platforms out there, you don't want to pay for all of them, each platform will have a learning curve, security model and risks
- ☐ Think about regulatory compliance
- ☐ Plan if you are looking to "bridge the gap" or move to a remote first workforce going forward
- ☐ Be cognizant of the risk of shadow IT and encourage your team to communicate holes in your toolset

Employees

- ☐ Set expectations, making sure that employees understand their responsibilities as they move to a remote workforce, and managers understand the complexities of entire families working from home
- ☐ Implement a quick daily team meeting to keep everyone on track and in touch
- ☐ Document process changes
- ☐ Video meetings can bring the team together in a highly effective manner if you learn to use them properly

Customers

- ☐ Communicate any major changes in workflow, policy or expectations to your customers

Security – Company Owned Devices

- ☐ Provide guidance to employees via company policy for IT assets
- ☐ Secure physical access to your laptop or IT equipment at all time – both from theft and chocolate milk spills
- ☐ Lock your computer when you walk away from it, and don't share company IT equipment with others
- ☐ Don't print sensitive materials in shared spaces - don't print if you don't need to and always secure printed materials
- ☐ Understand how backup works on remote IT assets at your company, what is being backed up and how often

Security – Personal Devices

- ☐ Update your security software regularly
- ☐ Use secure networks and your company provided VPN if approved
- ☐ Do not store business data on your personal device
- ☐ Use separate password protected accounts for administrators and each user on shared workstations, separate work and personal accounts
- ☐ Require screen lock with a timeout
- ☐ Enable device encryption if possible
- ☐ Do not use devices/software that are not approved by company policy

Social Media/Email

- ☐ Don't put anything on social media that you wouldn't share with your closest competitor or largest customer
- ☐ Do not use personal email or other accounts for company business
- ☐ Think before you click – attackers are working harder than ever to compromise businesses and individuals