RETURNING TO THE OFFICE AFTER COVID-19

IT Checklist for SMBs

■ Evaluate any new technology deployed during the crisis.

The tools your employees used to work remotely may or may not be required when you return to the office. Create a list, including any new devices, and decide if they stay or go. Evaluate how the new tech was implemented, determine what worked and what fell short, and if you still need all of the licenses you purchased. Examples include new Office 365 licenses, Zoom, new laptops, etc.

■ Catalogue items that were removed from the office.

Protect your business and intellectual property by ensuring any devices, technology, files, folders, contracts, customer lists, and documents, etc. are properly returned to the office. This list may include electronic files left on the employee's personal workstation or device.

■ Run an audit on your remote working tech.

For any employee who will continue to Work From Home (WFH), audit the tech they will be using. Determine if the tech is appropriate, secure, and is sufficient to enable optimal productivity.

■ Run an audit on your office workstations.

An audit will help you determine if the workstations are properly patched with the latest OS and other critical updates. Leverage your remote monitoring and management (RMM) tool to deliver the proper patches.

■ Document a list of employees who used their personal computers to WFH.

Develop an appropriate action plan to ensure the ongoing use of personal computers or devices complies with your company's security standards. Consider requiring your employees to change the passwords on any personal devices.

■ Review your Business Continuity + Disaster Recovery (BCDR) plan.

What can be improved upon? What worked well? Were you able to easily transition from the office to remote working? How was your business impacted during this crisis? Update your BCDR plan accordingly.

■ Evaluate your IT service providers.

Identify any managed service provider (MSP) that was not able to achieve their SLAs, and determine the cause. Pay particularly close attention to those critical MSPs and how they performed during the crisis.

■ Conduct a gap analysis.

Document the technology gaps that were exposed during the crisis and create a plan on how to address them.

■ Schedule regular BCDR testing plan.

This should be a routine part of your business. But given this recent crisis, regular Business Continuity and Disaster Recovery testing will be even more crucial moving forward. Don't get caught unprepared.

kbr keeping business running

0191 492 1492 info@kbr.co.uk www.kbr.co.uk