TeamLogicIT®
Your Technology Advisor

CHECKLIST

REMOTE WORKFORCE

For many companies, asking employees to work from home has become the new normal. Below is a checklist to help you understand your readiness to provide a highly secure and stable environment for your remote workers as well as your business.

READINESS

- [ ] Review employee hardware needed to work remotely.
  - Computer / keyboard / mouse / monitor(s)
  - Broadband Internet/Wi-Fi
  - Printer / scanner
- [ ] Verify that employees have a reliable broadband Internet connection (50Mb x 5 Mb or higher to support multiple endpoints and video calls/VoIP).
- [ ] Set up network connectivity for each employee (LAN-hardwired connections, reliable dual-ban wireless router, secure and segregated connections to IoT, TVs, PCs, etc.).
- [ ] Ensure secure and reliable access to all critical applications and data via VPN from employees' home office and that all licenses are up to date and adequate.
- [ ] Set up and put in place web conferencing and collaboration tools.
- [ ] Check remote access to the business phone system either through VoIP/softphone or other solution.

POLICIES

- [ ] Review your bring-your-own-device (BYOD) policy to manage personal devices that remote workers may use at home for business purposes.
- [ ] Make sure your remote work and network access policy is clear, enforceable and up to date.

  Date of last update: _____
- [ ] Enable remote access for each device employees will be using.
- [ ] With hackers targeting remote environments, and increased COVID-19-related phishing scams, the risks for security breaches are high. Consider the following policies for your incident-response plan:
  - Acceptable use policy
  - Data breach policy
  - Password protection policy
  - Disaster recovery plan policy

SECURITY

Remote workers can expose systems and networks to the risks of cyberattacks and breaches. It is important to ensure that the right security measures are in place to support secure IT operations.

- [ ] Use multi-factor authentication (MFA) to improve login security.
- [ ] A secure VPN should be installed on your servers.
- [ ] Ensure all operating systems, browsers and applications are patched and up to date.
- [ ] A monitoring and remote access tool should be installed to ensure proper authentication.
- [ ] System access protocols should be followed.
- [ ] Have employees review your security awareness training.

If you would like assistance in putting a work-from-home technology plan in place, contact us, and we will walk you through the appropriate solution.

Move forward ***together*** with **The Color of Confidence®**.

TeamLogic IT of NEPA • (570) 260-2500 • ScrantonPA@TeamLogicIT.com
3218 Pittston Avenue • Scranton, PA 18505 • TeamLogicIT.com/ScrantonPA