Remote Work Organizational Checklist

Each organization has unique variables that need to be factored in to help identify any remote work solution(s) that will fit their individual needs. This checklist is intended to help guide an organization to think through the variables associated with how to enable their team to work remotely as securely and productive as possible. Here are some recommendations and infrastructure considerations to support remote work.

VPN Connections

If your staff needs to connect to the office remotely, your firewall needs to be configured (if not already) for accepting VPN connections. Additionally, VPN connections are licensed by the number of concurrent connections.

- Action: Additional Licensing or configuration may be needed to enable additional remote access – contact Cervisys for assistance.
- Action: Distribute instructions to team to download VPN client and how to connect to the VPN.

Internet Connection

If more of your team is working remotely, that will put additional stress on your Internet connection. You may be able to contact your Internet Service Provider(s) (ISP) and ask if they can increase your bandwidth. Sometimes that can be done quickly depending on the type of connection(s) you have.

- Action: Additional bandwidth may be needed – contact your ISP for upgrade options.

Application Remote Access

Many applications can work over a VPN connection or are accessible via a web browser - like Software as a Service (SaaS) applications. If not, you may need to look at connecting your team to the application via a Remote Desktop/Terminal Server or to an internal desktop to maintain continuity. If the latter applies to you, please contact Cervisys to discuss further and formulate a plan. Additional configuration and/or licensing may be required to enable access.

- Action: Additional licensing and/or configuration may be needed to enable this type of remote access – contact Cervisys for assistance.

Internal & External Communications

Identify the preferred method for internal (email/Teams) and external (phone system/cell phones) communication and any contingencies needed for continuity.

- Action: For external communication, consider forwarding extensions/direct dials to cell phones, using a softphone (if your service has this feature), and potentially editing your auto attendant message to inform callers of this interim status.
- Action: For internal communication, encourage the use of Teams (or another audio/video tool) to keep your team connected.

Educate Your Team Regarding Increased Risks of Working Remote

The most significant infrastructure security risk in any organization is the human element – your team. Your team is going to be at greater risk working beyond the confines of your office network, and Bad Actors have been exploiting this risk. For example, malware has been found on a COVID-19 tracking map taking advantage of individual curiosity.

- Action: Educate - or reinforce the education to - your team to be on the lookout for suspicious emails and links in emails or on websites.