Remote Working checklist for IT admins

" This checklist covers the key areas an IT admin must focus on to secure and maintain a remote workforce. "

EMPLOYEE ONBOARDING

☐ Have you taken inventory of the equipment employees will require to perform their tasks remotely? (e.g., laptops, smartphones, headsets,)

☐ Have you enforced a streamlined way to securely deploy company devices to remote employees?

☐ Have you set up user accounts and synchronized relevant data including emails, calendars, and contacts for your employees?

☐ Have you ensured that employees have 24/7 access to an uninterrupted internet connection?

REMOTE COLLABORATION & COMMUNICATION

☐ Do employees have access to online tools that let users collaborate and work on tasks remotely? (e.g., Office 365, Google Workspace)

☐ Have you evaluated and set up remote communication platforms to assist employees with collaboration? (e.g., Microsoft Teams, Slack)

☐ Do you have tools in place that enable employees to keep in touch with customers virtually? (e.g., Ring central, Zoom)

MANAGING PRODUCTIVITY & WORK HOURS

- ☐ Do you ensure remote employees will be available for collaboration during the specified work hours?
- ☐ Do you encourage employees who work remotely to take breaks in line with the company's guidelines?
- ☐ If required, do you possess the ability to lock down remote devices to a specific set of apps and resources during work hours?
- ☐ Have you implemented a system that records and maintains time and attendance reports for employees who work remotely?

DATA PROTECTION

- ☐ Do you ensure that your remote workers' personal and sensitive data is kept confidential and secure?
- ☐ Do you possess the ability to remotely lock, or in worst cases, wipe the company data stored on remote devices?
- ☐ Does your data protection policy comply with regulatory guidelines such as GDPR and HIPAA?
- ☐ Have you made it mandatory to require a VPN to access company apps and resources?
- ☐ Do you authenticate employees with MFA/passwords/biometrics, before granting them access to the company's apps and resources?
- ☐ Are employees trained in identifying and avoiding social engineering attacks, phishing, and other security threats while working remotely?

ENDPOINT SECURITY

- ☐ Have you enforced restrictions and security configurations on company devices?
- ☐ Are your work devices updated to the latest patches and operating systems?
- ☐ Have you enforced encryption and password policies on your remote devices?
- ☐ Have you enabled firewall and installed antivirus software on company devices?
- ☐ Have you blocked your remote employees from accessing unproductive apps and resources?
- ☐ For employees who use personal devices to access company resources, have you enforced BYOD policies to secure sensitive data on devices?

REMOTE MONITORING

- ☐ Do you regularly monitor the health and status of company devices?
- ☐ Are you able to track the real-time location of company devices, and enable workers to check in with their location data?
- ☐ Do you possess the ability to lock down devices if they wander outside the specified work zones?
- ☐ Do you perform regular checks to verify that employees adhere to company policies?

REMOTE TROUBLESHOOTING

- ☐ If required, do you possess the ability to remotely view and/or control the screen of work devices?
- ☐ Can you broadcast important messages to your remote devices?
- ☐ Can you remotely ring devices, see their location, and if necessary, clear their passwords?
- ☐ Do you possess the ability to power off, or restart devices remotely?
- ☐ Can you remotely push scripts to your devices and automate time-consuming tasks such as creating folders, moving files, etc?

ANALYTICS AND REPORTING

- ☐ Do you maintain important employee details (including team, designation, and roles), and the resources they are assigned with?
- ☐ Do you maintain a system to edit and manage device attributes and information?
- ☐ Do you keep a record of the applications installed on your company’s remote devices?
- ☐ Do you maintain and manage a history of the location details of your remote devices?
- ☐ Do you maintain a record of the network data used by your managed apps, and their corresponding expenses to the company?