Nessit

Remote Readiness Checklist

Consider the following:

	YES	NO
Have I determined which staff members or roles can work remotely, those that can't work remotely and those where remote work may be possible with some changes?	☐	☐
Does my team have a plan in place to address systems and equipment needs of employees who may not be set up to work from home?	☐	☐
Do all devices that will be used remotely have the latest version of their operating software, security software, and line of business applications? Have we implemented two-factor authentication when logging into sensitive applications?	☐	☐
Do my remote employees have access to and know how to use a business-grade VPN? Have I purchased enough licenses for all the employees working remotely?	☐	☐
Does my team know about emerging threats tied to the COVID-19 coronavirus? This includes critical reminders like: - Minimum necessary rule – only use confidential and personal information as needed to complete the employee's assigned tasks. - Being aware of phishing attacks, which are particularly concerning now as a threat-actors are using the coronavirus as part of their attacks. - Knowing where to report a data incident. - Following instructions for system updates and security patches. - Saving company data only on company managed equipment, and not personal devices.	☐	☐
Does my team have a secure, unified videoconferencing & collaboration platform to use?	☐	☐
Have I ensured there are backups of our services so staff can keep working when extra network traffic causes primary services go down? Do employees know where to backup data to ensure business continuity in the event of device failure?	☐	☐
Does my company have guidelines in place for remote employees, including proper use of company assets and security guidelines? Does my team know about them?	☐	☐
Is my IT infrastructure and network designed to handle increased remote traffic?	☐	☐
Does my company have a plan in place to regularly check in with remote staff to confirm they're comfortable with working remotely and have the tools they need?	☐	☐
Have I reviewed and confirmed that existing policies and customer agreements allow us to work remotely when feasible, prudent, and contractually permissible?	☐	☐