Network Compliance Checklist for Remote Work

	Checklist item	Actions to take
□	Remote work program management	Establish a remote work program with senior management approval. Establish teams to manage it, such as IT and HR.
□	Establish remote work policies for employees and nonemployees	Prepare remote work policies that address the following areas: • Device technology. • Network technology. • Security technology. • Data management. • Network management. • Testing. • Employee training and awareness. • Remote access to company resources. • Help desk support. • Incident response. • People management. Also schedule periodic policy reviews.
□	Establish remote work procedures for employees and nonemployees	Develop, approve and document procedures for the following areas: • Remote work setups. • Use of personal devices and how they're configured. • Use of company-prepared systems in lieu of personal devices. • Equipment configuration. • Network configuration. • Security management. • Remote access to company resources. • Data backup and recovery. • Data protection. • Help desk support. • Incident response. Schedule periodic procedure reviews.
□	Remote network services	Consider the following areas: • VPNs. • Internet access. • Access to internal company networks. • Access using cloud services.

	Checklist item	Actions to take
		• Access via a VoIP system.
□	Primary network security	Consider the following areas: • End-to-end encryption. • Anti-phishing and malware software. • Intrusion detection and prevention systems (IDS/IPS). • Firewalls. • Network monitoring systems. • Network diagnostic systems. • Patching. • Penetration testing.
□	Remote network security	Consider the following areas: • End-to-end encryption. • Anti-phishing and malware software. • Ransomware software. • IDS/IPS. • Firewalls. • Antivirus software. • Patching. • Penetration testing.
□	Network performance management	Review network performance 24/7 if possible, considering the following factors: • Sufficient bandwidth. • Data throughput. • Latency. • Disruptions. • Local carrier outages. • WAN carrier outages. • ISP outages. Ensure that device patching is up to date. Also check that sufficient licenses are in place if VPNs are used. Review carrier disaster recovery plans in case of an outage.
□	Patch management	Ensure that patching is completed when needed. Establish a patch management program to ensure patching is performed.
□	Endpoint security	Ensure that devices have the most current security software installed, including the following: • Encryption. • Antimalware.

	Checklist item	Actions to take
		• Anti-ransomware. • Antivirus. • Firewalls.
□	Use of personal equipment (BYOD policies)	Ensure that IT staff reviews devices and that security apps are installed to comply with company security policies. Run tests to confirm the security is set up correctly. Periodically conduct penetration tests to ensure compliance.
□	Use of company equipment	Configure devices for remote use (e.g., laptops) with the proper security and access control software and policies. Run tests when devices are installed to verify controls. Periodically perform penetration tests to ensure that company devices have not been compromised.
□	Remote access controls	Ensure that remote access is based on company policy that includes the following: • Passwords. • Role-based access. • Multi-factor authentication. • Protocols.
□	Encryption	Deploy encryption based on company policy, such as end-to-end encryption, encryption for data at rest and encryption for data in motion. Enable security provisions for devices used remotely.
□	Collaboration resources	Ensure that the following tools are installed correctly and have security enabled: • Collaboration tools for video, such as Google Meet, Microsoft Teams and Zoom. • Messaging and text tools, such as Slack. • Email, such as Outlook and Gmail. • File sharing, such as Dropbox, Google Drive and OneDrive.
□	Data protection	Ensure that data can be stored in a secure environment, so only individuals with proper authorization can access it. Establish data protection and data management policies to support this.
□	Data backup and recovery	Back data up to secure local or remote storage facilities, especially personally identifiable information. The data must be easily recoverable and

	Checklist item	Actions to take
		retrievable in an emergency where data might have been stolen or damaged in a cyberattack.
□	Incident detection and response	Remote users must be able to contact a help desk or other resources if they experience system or network problems, or if they suspect a security breach. Establish formal incident response and help desk protocols and include them with remote work policies.
□	Employee and nonemployee training and awareness	Regularly send information to remote workers about technical or other developments. Establish training programs for remote workers who use company devices and employee-owned devices on how to access company resources. Diagnose any problems that emerge from training. Incorporate training as part of employee onboarding and update them periodically or when technology changes occur.
□	Audits	Coordinate with internal or external auditors when scheduling remote work audits. Gather evidence using the following tools: • Penetration testing. • Network and system logs. • Remote monitoring systems. Identify controls to be audited and examine the following areas: • Remote user compliance with policies. • Data protection compliance against key standards and regulations. • Trouble reports and security breach reports.
□	Testing	Run tests on company and employee devices to ensure proper operation. Test all new network resources before deploying to remote workers.
□	Incident response	Establish a process for responding to remote workers who report problems with a device, access to network services or access to company resources. Coordinate with a help desk or other trouble reporting service.
□	Disaster recovery	Establish a protocol for communicating information to remote employees about disruptions at the main company location or data center. Provide guidance on steps to take when it's safe to resume normal

	Checklist item	Actions to take
		operations. Tell remote workers to contact the help desk to report any problems with remote locations. Document procedures for remote workers to respond to a local disruption, similar to technology disaster recovery plans for headquarters and other major office locations.