NETWORK INTELLIGENCE
Global cybersecurity provider

Remote Working - Cybersecurity Checklist

#	Category	Sub-category	Checks	Remarks
1	End User device security - Laptop/Computer	System updates and patches	Operating system version - ensure it is a supported version	
2			Check for missing patches and security updates	
3		Secure Antivirus Configuration	Is antivirus installed on the end user device?	
4			Is antivirus updated with latest definitions?	
5			Is antivirus scan run regularly on drives and removable media? If yes, then are there any high level security issues reported?	
6		Use of pirated applications	Are any pirated applications installed on end user device?	User with personal Laptop
7			Check if OS is pirated	User with personal Laptop
8			Are there any potentially unwanted applications and high-risk applications installed on laptop?	User with personal Laptop
9		Use of freeware tools	Are their any freeware tools installed. If yes, then for what purpose?	
11		Data Security	Is important data backed up regularly and backups are stored securely?	
12			Is sensitive information such as PII, company confidential data well-protected?	
13			Are sensitive drives and files encrypted?	
14		Data Loss Prevention (DLP)	Is a data loss prevention (DLP) solution/agent installed on endpoint?	
15			Are DLP policies configured to protect organizational data over unknown network? (such as home network, public network, etc.)	
16			How DLP solution restricts storage or transmission of data to an unknown source such as USB, personal cloud storage, personal email, bluetooth file transfer, etc.?	
17			Is DLP solution configured to send alerts on any policy violation or potential data loss?	
18			Is it possible to disable DLP agent on an endpoint system?	
19			If there is no DLP solution in place, then is endpoint configuration protecting sensitive data files using encryption?	User with personal/organization laptop without DLP
20			Are there any restrictions to prevent copying of sensitive files to removable media?	User with personal/organization laptop without DLP
21			Is there use of virtual desktop infrastructure (VDI) or private cloud to limit employees' personal device usage only for accessing company network?	User with personal Laptop
22		Login Security	Is system password meeting the complexity standards?	
23			Is PIN or other biometric security or multifactor authentication mechanism used by user on End User Device?	
24		Bring your own device (BYOD)	Is there a "Bring your own device" (BYOD) policy in place which will ensure secure usage of personal device	
25	End User device security - Mobile		Is a Mobile Device Manangement solution installed on the device?	
26			If yes then which applications are whitelisted / blacklisted for installation?	Some applications like Tiktok, Mi etc (which gathers user info, device type, applications installed etc.) can leak out senstive data

27			What premissions are assigned to those applications?	
28	Network Security	VPN Secure Configuration - Process Security	What is the process of adding a user to the VPN user group	
29			What authorizations are required for a user to be added to the VPN user group	
30			What is the process when a VPN user leaves the organization	
31			What is the change management process around the VPN	
32			What logs of the VPN are enabled? What is the monitoring mechanism of the same	
33			What is the failover option if the VPN server fails? Is it a single point of failure or is there some redundancy built somewhere?	
34			Is there a user rights review process, where they periodically review the list of users?	
35			Do the dept. heads verify the list or above process? Do they verify and approve privileges assigned to each user?	
36			Is there any access control mechanism to restrict users from accessing certain systems or applications?	
37			Is 2-factor authentication and tokens being used? What is the physical security process around the tokens	
38		VPN Secure Configuration - Technical Security	What type of type VPN is configured – SSL or IPSec	
39			In what mode is the VPN being used – Full or Web	
40			Is there any client application or browser plugin being used ?	
41			What kind of tunneling is being used – Full or Split	
42			Is there any source IP address restriction to connect to the VPN server	
43			What are the destination IP addresses of systems to which access has been provided?	
44			Is there any MAC address filtering of users connecting to the VPN server	
45			Has MAC address binding been implemented	
46			What is the maximum number of users who can connect at one time?	
47			Is there any port based filtering on the VPN server	
48			Is there any service based filtering on the VPN server	
49			Is there any groups created of all accessible servers. (is the entire system given access to via VPN)	
50			Is there any remote management system accessible on the system via VPN (or on any other system)	
51			Possibility of remote code execution on firewall or remote system	
52			Is the VPN client password stored securely by the application (in the registry, config files or memory)	
53		WiFi security	Check for default password for admin account on your home WiFi	
55			Ensure that the router has WPA2 encryption	
57		Remote Access Solution (VPN /Portal)	Where is the device placed in the organization network?	
58			What is the max number of connection load it can sustain?	
59			Is the bandwidth provided to the Remote access server meeting the work requirements?	
60		Virtual Desktop Infrastructure (VDI)	In case of virtual desktop infrastructure (VDI), is it updated with latest patches?	
61			Are secure/encrypted protocols used for VDI?	
62			Is multifactor authentication supported by VDI environment? If yes, then is it enabled for employees using VDI over personal devices?	
63			How is the corporate proxy restricting Internet access?	

64		Proxy Configuration	In case of personal laptop usage, share with the employee secure Internet practices.	
65	Sensitive Data Leakage	Usage by Family Members	Is the PC/laptop shared by family members of the employee?	
66			if yes, do they have seperate user accounts?	
67			How the data is segregated from other users data? Can other users access the sensitive data?	
68			How password policy is enforced?	
69			What are the parameters set for screensaver, idle timeout, multi-factor authentication?	
70			How physical security of any company asset is ensured?	
71			Are there any personal media storage devices in use? E.g. USB, Hard Drive, etc.	
72			Check if any other family member has admin level account on PC.	If yes, then the organization must consider to deploy a VM for having a controlled environment
73		General Awareness	Are employees trained on basic cybersecurity awareness?	
74			Was there any phishing activity conducted recently? If not then, are employees aware of such attacks and precautions to be taken?	
75			Are employees educated on data security, data handling procedures?	
76			Is there any policy or guideline defined for "work from home" or "teleworking"?	