Item		Remarks
Firewall		
You have a firewall in place to protect your internal network against unauthorized access	☐	
The password for your firewall device has been changed from the default to a strong one	☐	
Your default posture on all access lists, inbound as well as outbound, is “Deny All”	☐	
Every rule on the firewall is documented and approved by an authorized individual	☐	
Every alert is promptly logged and investigated.	☐	
You use only secure routing protocols, which use authentication	☐	
You promptly disable any permissive firewall rules that are no longer required.	☐	
Network Devices		
Purchase your network equipment only from authorized resellers.	☐	
Download firmware, updates, patches, and upgrades only from validated sources.	☐	
Ensure that all devices on your network are using WPA2 (Wi-Fi Protected Access II).	☐	
To maintain consistency and for ease of management, use standard configuration for each type of device.	☐	
Maintain a list of all your network hardware- include the device name, type, location, serial number, service tag, etc.	☐	
Disable those ports that are not assigned to specific devices.	☐	
Use physical or virtual separation that allows network administrators to isolate critical devices onto network segments.	☐	

Turn off all unnecessary services on routers and switches.	☐	
Regulate physical access to routers and switches.	☐	
Implement a robust password policy that ensures the use of strong password encryption.	☐	
If you are using SNMP (Simple Network Management Protocol), use SNMPv3. Do not use SNMPv1 and v2 as they are vulnerable to IP spoofing attacks.	☐	
Ensure that you use only OOB (out-of-band) for sending management traffic to devices.	☐	
Patch Management		
Use only licensed and supported software to ensure that vulnerabilities are investigated and patches made available.	☐	
Software updates and security patches must be installed as soon as they are available.	☐	
Unsupported software should be removed from devices capable of connecting to the internet.	☐	
Use a patch management solution. If you hire a Managed IT Services Provider, they usually offer patch management solution to fit your business requirements.	☐	
Malware Protection		
Anti-malware software should be installed on all computers and mobile devices	☐	
The anti-malware software must be kept up-to-date	☐	
Configure the anti-malware software to scan files and web pages automatically and block malicious content	☐	
Ensure that the software is configured to perform regular scans	☐	
User Account Management		
Create a unique user account and username for each individual	☐	

Implement a robust password policy to ensure all users have strong passwords	☐	
Implement 2FA (Two-Factor Authentication)	☐	
All user accounts and their privileges must be documented and approved by an authorized individual	☐	
Admin accounts should be used only for performing admin tasks	☐	
User accounts, especially those with admin accounts must be removed when no longer required.	☐	
Use only one approved remote access method to maintain consistency.	☐	
Give remote access only to authorized users. Give unique credentials to each user instead of using a common account.	☐	
Use virtual private networks (VPNs) for remote access to secure your device and connection when using public networks.	☐	
Set up a guest WiFi ,which is segregated from your internal network, for visitors and employee-owned devices.	☐	
Educate your employees about cybersecurity risks and attacks they are vulnerable. Teach them how to identify phishing and steps they need to take if infected.	☐	
Email and Internet Access		
Use mail filters to protect against spam, malware, and phishing.	☐	
Configure your devices to reject any directory harvesting attempts.	☐	
Use an email filtering solution to filter both inbound and outbound messages. This will protect your users as well as your customers.	☐	
Ensure that your anti-malware software scans all content including streaming media.	☐	
Implement an Internet monitoring solution to provide your users with secure Internet access.	☐	

Block any outbound traffic that can potentially be used to go around your Internet monitoring solution.	☐	
IT Policy		
Perform penetration tests to identify vulnerabilities.	☐	
Use phishing audits to test the preparedness of your users against phishing attacks.	☐	
Make encryption mandatory for all mobile devices that leave your office premises.	☐	
Perform vulnerability scans on random samples of your workstations to check if they are up-to-date.	☐	
Backup all data, which is critical for your business, regularly.	☐	
Perform test restores to verify that your backups work properly.	☐	
Disable Wireless Protected Setup (WPS) on all wireless devices.	☐	
Disable the Universal Plug n Play (UPnP) option.	☐	
If you have a BYOD (Bring Your Own Device) policy, ensure that you use an MDM (Mobile Device Management) solution.	☐	
When granting permission to file share, the default must be “read-only”. Restrict “full control” to admin accounts.	☐	
Establish procedures for onboarding and off-boarding employees.	☐	