

Cybersecurity Health Check Questionnaires for Small and Medium Businesses

Please answer the following questions to the best of your knowledge. These questions will assist with information required to provide your company with a suitable cybersecurity compliance. However, having compliance does not guarantee data protection.

What is the nature of your business? _____

How many employees do you have? _____

Are you a home-based company? If yes, is any of your home devices/appliances connect to the Internet? Please provide us details. (name of the device(s)/appliance(s)) Do you have a password for your device(s)/appliance(s)?

Please mark (X) to all that apply. Some of the questions may sound repetitive. Please answer to the best of your knowledge.

Item	Function	Category	Yes	No	Not Sure
1	Identify	Are you aware of a risk of connecting unauthorised devices to your company's network?			
2		Do you allow your visitors to connect to your network while they were having a meeting in your office?			
3		Does your company have a data privacy policy in place?			
4		Does your company conduct Information Security Audits or Risk Assessments?			
5		Are you aware of a Risk Management Strategy in your company?			
6		Do you use cloud infrastructure?			
7		Are you familiar with the word "Phishing" and "Spear Phishing"?			

8	Protect	Do you have password protection for all your important files?			
9		Are you familiar with system firewall? Do you have any firewalls?			
10		Do you participate in any Information Security or Cybersecurity Awareness Sessions/ Trainings?			
11		Do you have a Clear Desk Policy?			
12		Are you aware of any Information Protection and Procedures in your company?			
13		Do you have administrative and privilege access to all systems and data?			
14		Do you run any updates and conduct regular maintenance on your firmware, Software and other devices			
15		Does your PC/company's devices have passwords or antivirus?			
16		Do you use the same password for all your devices?			
17		When was the last time you changed your password?			
18	Do you use multifactor authentications?				
19	Detect	Are you able to detect/identify any anomalies and suspicious events on your computer/network?			
20		Do you have Security Continuous Monitoring Systems?			
21		Will you disclose any information required by any Microsoft Technical Teams should they ring to provide technical support/advice?			
22	Response	Do you have a Cyber Crisis Communication Plan?			
23		Do you build rapport or have any collaboration with Information Security or Cybersecurity Companies?			
24		Do you have a mitigation plan posted in/around your office?			
25		Do you have a Cyber Incident Response Plan? If yes, have you tested your cyber incident response plan?			
26		Do you know who to report to should you experience a cyberattack?			

27	Recovery	Do you have a Data Breach/Cyber Disaster Recovery Plan?			
28		Do you have back up plan?			
29		Have you tested and fix any gaps in your Data Breach/ Cyber Disaster Recovery Plan?			
30		If yes, do you have media communication plan to update the public/customer and authorities about your recovery situation?			
31		Do you have continuous Security Awareness Training for your employees?			

Additional information:

Item No.: _____ Details: _____

Item No.: _____ Details: _____

For Official Use Only

Information compiled by:	Number of Employees in the company:
Interviewed by:	Date:
Additional information:	