Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

ICTSWITZERLAND ISSS Information Security Society Switzerland satw it's all about technology SNV SQS ASA | SVV

Cybersecurity quick test for SME

For SMEs who want to answer the full set of questions

How well is your company protected against and prepared for cyberspace attacks? Check now whether you meet the minimum standards for SMEs.

The risks of cyber-attacks are often greatly underestimated. This was shown by a 2017 survey of SME managers in Switzerland. Most SMEs feel well protected, although frequently too little is done to combat the threats.

This questionnaire enables your company to determine the current situation and shows you whether you are implementing the most important technical, organisational and employee-related measures for a minimum level of cybersecurity protection. If you answer «No» or «Don't know» to one or more questions, you will find additional information especially for SMEs at www.ictswitzerland.ch/themen/cyber-security.

	Yes	No	Don't know
1. Tasks, powers, responsibilities			
Have you determined who is responsible for cybersecurity in your company?			
Does the person responsible have the knowledge, skills and abilities necessary to deal with cybersecurity and does he or she receive regular training?			
Does the person responsible have the necessary hierarchical position and corresponding powers to implement cybersecurity measures?			
Are there guidelines for the secure handling of IT devices and data?			
Are these guidelines and cybersecurity measures consistently and systematically implemented and regularly reviewed?			

2. Raising awareness among employees, clients, suppliers and service providers			
Do your employees have company guidelines for dealing with email, digital data and the internet securely?			
Do the employees know and understand these company's cybersecurity guidelines?			
Do the employees implement the guidelines consistently and correctly?			
Are the employees regularly trained on cybersecurity, e.g. correct handling of email, or is their awareness raised?			
Does your company exchange information on cybersecurity with clients and suppliers? (They should do this quick test too.)			

	Yes	No	Don't know
3. Data protection guidelines			
Is the data on your systems (data stores, repositories, terminals and servers) encrypted?			
Do you hold or process personal data (in particular particularly sensitive data on health, religion, etc.) in electronic form?			
Are you aware of your duties in connection with the provisions on personal data?			
Are the current data protection regulations being implemented consistently and correctly in your company?			
Is physical access to the computer, server and network infrastructure in your company appropriately protected against access by third parties?			

4. Password guidelines and user administration			
Does your company have guidelines on the use of passwords?			
Are there guidelines according to which administration rights are systematically assigned?			
Are there guidelines that define which employees have access to what data?			
Are these guidelines implemented consistently and correctly?			

5. Up-to-date protection against malware			
Are your devices protected against malware (e.g. antivirus program, spam filter)?			

6. Configured and updated firewall			
Are your corporate network and IT systems protected by a firewall?			
Is your firewall updated regularly?			

	Yes	No	Don't know
7. Keeping devices and systems connected to the internet up to date (e.g. workplace systems, production facilities, building management systems, etc.)			
Do you use the automatic software update facility?			
In the case of devices and systems whose software is not automatically updated, are they regularly updated (e.g. by the manufacturer)?			
Are the mobile devices used in the company environment updated regularly?			

8. Protected and encrypted WLAN network			
Is your WLAN encrypted and protected?			
Is there a separate WLAN for employees and guests?			

9. Encryption of (data) transmission (e.g. VPN)			
Do you generally and continuously use secure and encrypted communication connections on the internet?			

10. Backups			
Do you apply a data backup process?			
Do you regularly check the functionality and readability of the backup?			
Is the storage of the backup physically separate (offline)?			

11. Minimum emergency response arrangements			
Are the immediate measures for an IT incident defined?			
Are the person responsible and the contact person in the event of an IT incident (e.g. malfunction, attack, etc.) defined and available?			

12. Outsourcing			
If you have outsourced IT services: Are points 1-11 of this quick test covered in the contract with the service partner?			

Version 2.0 | 02.04.2020