# Cybersecurity guide for SMEs


This guide has been developed to help SMEs achieve a minimum level of cybersecurity and thus better protect themselves from the most common cyberattacks.

SMEs are increasingly the target of cyberattacks, which can have serious consequences. Just a few important measures can help to achieve a minimum level of protection against cyberthreats. These measures are explained in this guide. The language used in the guide is clear, the steps are concrete and straightforward – specifically tailored to the needs of SMEs.

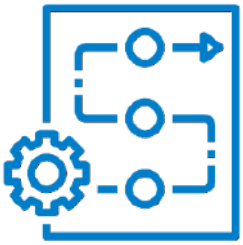
The guide complements the cybersecurity quick test for SMEs and follows the thematic structure it introduced. For a self-assessment of how your company stands in terms of cybersecurity, we recommend that you complete the quick test.

The guide and the upstream quick test for SMEs are part of the national strategy for the protection of Switzerland against cyber-risks. A specialist group developed the contents of the guide and tailored it explicitly to the needs of SMEs.

The partners involved in the development of the guide are jointly committed to ensuring that the Swiss SME landscape can protect itself as effectively as possible against cyber-risks. Read more about the specialist group on www.cybersecurity-check.ch.

# Overview

# Organisational and process security



## Why is it important?

In the event of a cyberincident, proper preparation and response are critical and determine whether and how quickly you can continue to run your business once it has occurred.

A quick and correct reaction can significantly reduce or even prevent damage. To achieve this, it is important to prepare your organisation to deal with these threats and to define appropriate processes, such as making regular backups of your data, selectively assigning access rights and preparing an emergency plan.

## What can I do?

- ☐ Secure your information by making regular **backups**.
- ☐ Ensure appropriate **user administration**.
- ☐ Prepare an **emergency plan**.

## How should I proceed?

**Secure information: Backup on a routine basis**

- Make a backup to an external hard drive at least once a week.
- Keep the backup in an external, protected location and separate from the network (offline backup).
- Check regularly whether the data can be successfully restored from the security storage location(s).

## Minimise areas of attack: Appropriate user administration

Successful user administration can make it more difficult for criminals to access particularly important information.

- Set up separate login accounts for admin tasks (particularly sensitive data, information and systems) and "normal" tasks.
- Give each user only the most essential access rights. This prevents attackers from gaining unlimited access to all systems.
- If possible, only use personal accounts (do not use accounts that are used by several users with the same user name/password).
- Define who has access to specific IT applications/information. Assign access rights according to roles (e.g. accounting/HR administration/secretarial/system admin/sales).
- Block individuals' user accounts/access data when they leave the company.

## Prepare for emergencies: emergency plan

Prepare an emergency plan so that you know what to do in case of an emergency.

- Identify systems that are critical in an emergency, e.g. address database, mail system, appointment calendar, etc. as well as private data and client data.
- Record who works with which system (names and telephone numbers).
- Define fallback levels (providing replacement PCs; equipping all workstations with at least two browsers; agreeing on response times and delivery deadlines with suppliers).
- Define the initial response in the case of an incident: disconnect the network connections (cable and Wi-Fi) of the affected systems.
- Define measures to quickly restore your systems.
- Define roles and responsibilities, i.e. who is to be informed and how in the event of an incident (e.g. in the event of a ransom demand or critical system failure):
    - Person/company to resolve the IT incident.
    - Person/company for immediate legal action. If, for example, personal data is affected, it is advisable to seek legal advice and/or contact a legal expert.

- Person/company for immediate communicative action.
- Person responsible for reporting the incident. This person will inform the nearest police station and the federal Reporting and Analysis Centre for Information Assurance (MELANI) www.melani.admin.ch. In cases of cyberfraud that involves financial loss, you are strongly recommended to contact your bank, the police and/or a specialised company immediately in order to stop any payments.

– Practise the emergency plan within your company.

# Human factor provides security

## Why is it important?

Despite all the technical resources, it is ultimately the employees who are the key to your company's security. It is therefore important that you and all employees are aware of the current dangers, are able to handle the technical equipment and comply with the most important rules.

## What can I do?

- ☐ Incorporate employee **awareness raising** into everyday company life.
- ☐ Use secure **passwords** to ensure the best possible protection for your applications.
- ☐ Define **user guidelines** for safe use of the internet and email.

## How should I proceed?

### Making security an issue: raising awareness

- Raise the issue of security, and in particular safe use of the internet within the company, on a regular basis.
- Organise basic training for your employees which includes the following content:
  - What are the benefits of IT security?
  - What are strong passwords? (see below)
  - What does safe use of the internet and email mean? (see below)

## Best possible protection for your applications: strong passwords

- Choose secure passwords, i.e. use passwords that are as long as possible and include at least 12 characters.
- Use a password manager and automatically generated passwords.
- As an alternative, use a passphrase: Choose a sentence that only you know and nobody else can easily guess. From this sentence, take the first one or two letters of each word to form a password. Be careful not to use common sentences or phrases like book titles, turns of phrase, etc.
- Do not use passwords more than once, i.e. use a different password for each service such as your email account, online banking, accounting software, CRM applications, etc.
- Use two-factor authentication if possible (e.g. Google Authenticator).
- Change impersonal passwords in the company when employees leave.

## Safe use of the internet and email: user guidelines

Define user guidelines for safe use of the internet and email. These can include the following points:

- Never give login details (username and password) to third parties at any time or under any circumstances.
- Only provide your credit card number(s) to trustworthy websites, e.g. make sure that https:// appears before the address in the browser.
- Do not download unknown programs from the internet.
- Use a smartphone as a hotspot instead of a public, unprotected Wi-Fi connection. This is particularly important for online banking. Unprotected connections are not secure and there is a risk that third parties may access your data.
- Be careful when receiving emails and pay particular attention to the following points:
    - In the case of dubious emails (e.g. unusual sender addresses, spelling mistakes, incorrect tone and logos), do not open attached documents or programs and do not click on links.

- In case of doubt, never disclose confidential information and try to contact the sender by other means (e.g. by telephone) to check if the email is legitimate.
- Also carefully check messages that come from someone you know or a senior employee in the company. Fraudsters may have access to that person's mailbox and send emails under their name.

# Security thanks to appropriate technical measures

## Why is it important?

Security vulnerabilities could allow unauthorised persons to gain access to your systems. Data can be destroyed and manipulated or your IT infrastructure could be manipulated for criminal purposes. Software updates remove these security vulnerabilities.

An up-to-date firewall can protect your computer from unauthorised access. Up-to-date antivirus software protects your data from viruses, worms and Trojans.

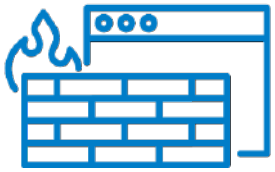
Criminals can read and even manipulate data traffic if your communications are not encrypted.

## What can I do?

- ☐ Use suitable **software** (e.g. firewall, antivirus software) to increase your security.
- ☐ Make sure you **update** your software **regularly**.
- ☐ Do not connect **outdated devices**, for which no software update is available, to the internet.

## How should I proceed?

**Increase security with technical tools: appropriate software and hardware**



- Update operating systems, firewalls and other applications regularly.
- Check your computer regularly for updates and make sure it is up to date to avoid security vulnerabilities.
- Use automatic update functions whenever possible. This also applies to all software products and devices connected to the internet, such as equipment, printers, building control systems, household appliances or smartphones.
- Disconnect devices for which no updates are available from the internet or disable them.

- Install up-to-date antivirus software and update it regularly (this is usually done automatically). A kTipp test from May 2019 recommends in particular the antivirus programs "Internet Security" from Bitdefender or Kaspersky and "Antivirus Pro" from Avira. The free software from Avast also scored well in the test.
- Protect your communications with good encryption (e.g. a virtual private network, or VPN).

# Cybersecurity as part of data protection

## Why is it important?

Your company is responsible for securely handling personal data and intellectual property. Loss of data or data protection violations can result in criminal consequences, high fines and serious reputational damage. These consequences could pose a threat to a company's existence.

Since 2018, the EU's new General Data Protection Regulation (GDPR) has been in force, which also applies in part to Swiss companies. GDPR affects Swiss companies and websites that handle data relating to EU citizens or have these as a target group. This also applies, for example, to websites that use cookies to evaluate the browsing activity of visitors from EU countries.

Cybersecurity and data protection go hand in hand: criminals can gain access to sensitive data through a cyberattack.

## What can I do?

☐ By adopting cybersecurity measures, you are contributing to the statutory compliance with the Data Protection Act.

## How should I proceed?

### Handle data in accordance with the law: data protection

- As soon as you process personal data (e.g. of clients or employees) in any way, you must protect it sufficiently (or only collect the data).
- Processing is defined as any handling of personal data, i.e. in particular obtaining, saving, storing, using, modifying, disclosing, archiving, deleting or destroying data.
- Check whether you are affected by GDPR: Economiesuisse online check, GDPR factsheet

# Security thanks to a suitable environment

## Why is it important?

If one of your suppliers or service providers is affected by a hacker attack, you may be affected too, e.g. if your own client data is lost. It is therefore important that third parties with whom you collaborate also implement the key cybersecurity measures.

If you outsource IT security to a third party, it is important that you keep a close eye on your provider and clarify the most important points with them.

## What can I do?

- ☐ Demand that **outsourcing partners and suppliers** implement minimum cybersecurity measures.
- ☐ When outsourcing **IT security services**, look for certificates and compliance with the key

## How should I proceed?

**Insist on security outside your own company: outsourcing partners and suppliers**

Go through the cybersecurity quick test with suppliers and service providers (outsourcing partners) and make sure that they also meet the same requirements that your company has to satisfy. Clarify the following points, among others:

- Are regular backups made and stored in an external location?
- Is there an emergency plan?
- Are there user guidelines in place and are they adhered to?
- Are there guidelines for user administration?

- Are employees made aware of cybersecurity issues (e.g. phishing emails, use of passwords)?
- Are operating systems, firewalls and other applications regularly updated?
- Is encrypted communication used?
- Is antivirus software used and regularly updated?

### Security when outsourcing security services: IT security providers

Make sure that the IT security provider meets the most important requirements: Go through the quick test with them or check whether they have an appropriate certificate (e.g. ISO 27001).

## To what we refer

### References and further information

MELANI: Information security checklist for SMEs

MELANI: Basic security measures

ISSS: Information security for SMEs

BNC: Cybersecurity and data protection

FDPIC: Data protection

Tagblatt: Datenschutzgesetz (article in German on the Data Protection Act)

kTipp: Antiviren-Software (article in German on antivirus software)

UBS: Phishing