POLICIES & GUIDELINES

Privacy & Security

Small Improvements Software GmbH

Revision: 11/2023

Content

Guideline on Data Protection & Information Security

1. Introduction

Small Improvements Software GmbH (SI) hereby adopts this guideline on data protection and information security in our company.

As a company, we process a large amount of sensitive data in order to fulfill our tasks and obligations towards our customers, contractual partners, service providers, public authorities and other third parties.

Almost all of the data we process on behalf of our clients is highly sensitive. Our entire business depends on us keeping our customers' data safe. If we ever lost a single customer's data, the news would spread and instantly erode trust in our company. No amount of savings could help the company recover. Data privacy is our topmost priority.

This guideline is intended to present the strategy, organization and objectives of data protection and information security in our company in a clear form.

2. Scope of application

This guideline applies to SI. It extends to all locations of SI as well as to the mobile workplaces. This guideline obliges all employees of SI to comply with the duties set out here. The guideline will be made available to employees in an appropriate manner in the version applicable at the time.

3. Objectives

The goal of this guideline is to ensure data protection and information security within the company. To this end, the company will take the following objectives into account when planning, implementing and during the operation of processes:

- legality
- transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- availability, integrity and confidentiality, resilience
- intervenability and processing in good faith ("fairness")
- accountability principle.

The consideration of these objectives is specified in separate guidelines.

In the concrete implementation of the objectives, the protective measures taken must be in an economically justifiable relationship to the need for protection of the data and information processed.

4. Organization of data protection and information security

4.1 Data protection officer

SI has appointed a Data Protection Officer (DPO). The Data Protection Officer is the contact person for the topic of data protection in the company. He advises, controls and supports the company management and employees with regard to the processing of personal data in the company. The further tasks result primarily from Art. 39 GDPR.

In the area of processing personal data, care must be taken to ensure that the Data Protection Officer is involved at an early stage in the planning and introduction of new processes in which personal data are also processed. The same applies to changes to existing processes.

A management system is set up in the company for the area of data protection. For this purpose, a process of continuous improvement is implemented in the company with the aim of coordinating the individual measures in the areas of data protection and information security in such a way that the objectives of this guideline are achieved.

5. Measures

The measures to implement these guidelines can take the form of technical and organizational measures. These include guidelines, company regulations or company instructions. These must be followed by employees.

6. Responsibilities

The company management assumes overall responsibility for information security and data protection in the company.

The responsibilities of the DPO and DST are already described above.

The IT officer implements the guidelines and other requirements on data protection and information security in his area of responsibility. He coordinates measures that have an impact on information security with the DST or the management.

The administrators implement the technical measures in coordination with the IT officer and contribute to optimizing information security by suggesting improvements.

Supervisors with personnel responsibility have the task of ensuring that the technical and organizational measures taken for information security are implemented with regard to the persons working in their area of responsibility.

All employees contribute to ensuring data protection and information security through their conduct. All employees are obliged to comply with this policy and all guidelines or instructions concerning them or their work when dealing with personal data. This applies in particular to requirements relating to the security of personal data.

In order to ensure data protection and information security in the company, all employees are obliged to report disturbances, security incidents and emergencies in the area of information security immediately and directly to the DST and the management.

Incidents in the area of data protection are to be reported by all employees to the DST and the management immediately upon becoming aware of them.

The respective guidelines of SI apply.

Project or process managers must consult the DST for all projects with an impact on the processing of personal data in order to ensure that data protection regulations can be complied with. Furthermore, all project or process owners are obliged to consult the DST for all projects that have an impact on information security in the company.

Suppliers, external service providers and other contractors must be obliged by separate agreements to comply with the data protection and information security requirements relating to them if they process data on behalf of the company or have the possibility of becoming aware of personal data or information of the company that is not classified as public.

7. Sanctions

A breach of this guideline may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

For supply companies, external service providers and other contractors, contractual penalty arrangements should be agreed where there are particular risks.

Guideline for the implementation of data protection measures

1. Introduction

Small Improvements Software GmbH (SI) processes personal data. SI is legally obliged to process personal data in compliance with the applicable data protection regulations.

The relevant legal provisions are the General Data Protection Regulation (GDPR), the Federal Data Protection Act and, where applicable, sector-specific legal provisions.

Every business process that involves the processing of personal data must be checked by SI for compliance with the legal requirements.

In addition, the data protection officer of SI is responsible for checking compliance with the legal tasks.

In order to ensure the legal conformity of data processing in the company, SI makes specifications for the establishment, testing and implementation of data processing processes through this policy.

In addition, this policy supports the creation and maintenance of the Directory of Processing Activities within the meaning of Article 30 of the GDPR. The same applies to the support in connection with the examination of whether (and, if necessary, how) data protection impact assessments within the meaning of Art. 35 of the GDPR are to be carried out.

Furthermore, SI shall comply with any notification obligations pursuant to Art. 33, 34 DSGVO.

2. Scope of application

This policy applies to employees who are responsible for setting up or carrying out processing of personal data at SI or for a processing operation themselves as “owner”.

This policy applies to all locations of SI.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

The purpose of this policy is to help ensure compliance with the law on the processing of personal data.

4. Principles for the processing of personal data

The following processes and principles must be complied with when processing personal data in accordance with Art. 5 GDPR:

Personal data must

1. be processed on the basis of a legal basis or consent, fairly and in a way that is comprehensible to the data subject (“lawfulness, fair processing, transparency”);
2. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (‘purpose limitation’);
3. adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing (“data minimisation”). That means we make sure to only collect the least possible amount of data needed to achieve essential business goals. We never collect data on the grounds that it might be useful in the future.
4. be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes of their processing are erased or rectified without delay (“accuracy”)
5. be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (“storage limitation”);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organizational measures (“integrity and confidentiality”);

If employees have any questions regarding the application and interpretation of these principles, they can contact the Data Protection Officer and/or the Data Protection Team (DST).

5. Exceptions

SI may allow exceptions to the principles stated under point 4 in justified cases. Exceptions are to be reviewed by the DST and agreed with the company management. Approved exceptions are to be documented including a justification.

6. Records of processing activities

SI shall keep a register of processing activities and - insofar as SI acts as a processor - also a register of processing activities for processors within the meaning of Article 30 (2) of the GDPR.

The directory of processing activities is maintained by the DST. The DST shall ensure that the processing registers are regularly updated.

All employees who are responsible for setting up or carrying out processing operations of personal data at SI or for a processing operation themselves as the “owner” are obliged to notify the DST in the event of a planned set-up or change of processing operations and/or business processes. The notification shall be made by e-mail to the DST or the DST members.

7. Data protection impact assessment

The DST will assess each new notified processing operation to determine whether it is likely to present a high risk to personal data. The same applies to changes in processing operations.

If the risk is likely to be high, the DST will recommend to the management that a data protection impact assessment (DPIA) be carried out. The company management decides on the “whether” and “how” to carry out the DPIA.

In principle, the respective processing may only be started after the DPIA has been carried out and the corresponding approval has been given by the company management.

The DPIA can be carried out by the DST. The DPIA can also be carried out by external, competent persons. The Data Protection Officer (DPO) is available to advise on the performance of the DPIA upon request.

The result of the DPIA is communicated to the company management. The management decides on the release of the processing operation.

If the DPIA shows that the risk associated with the processing operation cannot be contained by technical and organizational measures, the management shall decide whether prior consultation with the supervisory authority within the meaning of Article 36 of the GDPR is required.

8. Notification obligations in the event of data protection breaches

The DST shall promptly investigate any incident or notification (“Incidents”) of a personal data breach.

Each Incident shall be documented by the DST in the data protection tool. In doing so, the time of knowledge, the statement of facts and the measures taken are documented.

For each incident, it must first be assessed whether a personal data breach has occurred and whether the breach is likely to lead to a risk for the data subjects. In the risk assessment, the amount of damage and the probability of occurrence are the decisive factors.

In the event of a risk, the DST must immediately inform the company management and ensure that a report is made to the Data Protection Supervisory Authority responsible for SI within 72 hours of becoming aware of the incident.

If the 72-hour deadline has already passed, a report will nevertheless be made to the supervisory authority as soon as possible. This report must then be accompanied by a justification for the delay. The notification must be coordinated with the company management in advance.

The notification must include in particular

- a description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer or other contact point for further information;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed by the data controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

If the above information cannot be identified or compiled within the 72-hour period, a notification must nevertheless be made to the supervisory authority. The above-mentioned contents must then be submitted to the supervisory authority without delay.

If the personal data breach is likely to pose a high risk to individuals affected by the incident, the DST shall notify the affected individuals of the breach without delay. The DST will coordinate the notifications in advance with the company management and, in doing so, will in particular consider any exemptions pursuant to Article 34 (3) of the GDPR.

Insofar as SI processes personal data on behalf of other companies or organizations, a notification of an incident must be made immediately to the party ordering the data processing. With regard to the time and type of notification, it must be checked immediately after becoming aware of an incident in the relevant order processing contract with the client when and how the notification to the client is to be made.

9. Training measures

All employees of SI shall be familiarized with the legal provisions on the processing of personal data in data protection training promptly after commencing their work for SI and thereafter on a regular basis.

All employees who are responsible for setting up or carrying out processing of personal data at SI shall ensure that the employees who have access to personal data via this processing have been trained on data protection beforehand.

For this purpose, an online training tool is provided to ensure that employees are trained in accordance with the guidelines. In addition, classroom training or online webinars may be provided.

10. Sanctions

A violation of these guidelines may constitute a breach of duty under the employment contract and be sanctioned accordingly.

Guideline for the implementation of data subject rights

1. Introduction

The General Data Protection Regulation (GDPR) contains in Art. 12 and the following of the GDPR the rights of the persons affected by a processing of personal data, which have to be complied with by Small Improvements Software GmbH (SI).

In order to ensure the protection of these data subject rights, measures for the implementation by employees of SI are defined in this policy.

2. Scope of application

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

The purpose of this policy is to help ensure compliance with the law for the protection of the rights of data subjects.

4. Information obligations

The Data Protection and Information Security Team (DST) shall maintain the register of processing activities. The DST shall ensure that, for each processing operation in the processing directory, care has been taken by the “owner” of the processing operation to ensure that data protection information for the data subjects is available to the required extent and is also made available to the data subjects in an appropriate manner.

The information must also be checked by the “owner” to ensure that it is up to date in the event of changes to the processing.

The type and scope of the provision of information must be agreed with the DST.

5. Rights to information, deletion, objection and other data subject rights from Art. 15-22 GDPR

Every person can assert their data subject rights in accordance with Art. 15-22 GDPR against SI.

This includes in particular the right to information, correction and deletion of personal data as well as the right to restriction of processing and the right to objection to the processing of data (e.g. also against the use of data for advertising purposes).

All employees of SI are obliged to forward a claim for information, correction, deletion or an objection asserted by a data subject to the DST immediately after receipt of the notification. The forwarding can also take place, for example, by e-mail to the e-mail address of the DST.

The DST will document the request and respond to the data subject without delay, but no later than within one month of receipt of the data subject's notification by SI. The DST will inform the management of difficult or extensive requests from data subjects.

When responding to requests from data subjects, the DST must ensure that, prior to providing information to the data subject, it has been verified that the person is who he or she claims to be in order to prevent personal data from being disclosed to unauthorized persons. In the case of information being provided by e-mail, the consent of the data subject to the provision of the information by e-mail must be obtained in advance. In the absence of consent, the information shall be provided in writing.

6. Deletion of requests from data subjects

The documentation of enquiries from data subjects as well as their replies shall be kept for three years from the last correspondence with the data subject.

After the expiry of three years, the DST shall examine whether further storage of the documentation is necessary or whether it can be deleted. In particular, any existing legal claims or the defense against alleged or asserted legal claims shall be included in the examination of the necessity.

For the purposes of better implementation, this examination may be carried out after the above-mentioned period of three years at the end of each calendar year.

7. Sanctions

A violation of these guidelines may constitute a breach of duty under the employment contract and be sanctioned accordingly.

Guideline for dealing with service providers

1. Introduction

At Small Improvements Software GmbH (SI), service providers and other contractors (hereinafter generally referred to as “service providers”) may also be commissioned to perform services.

Our core data lives in the highly secure Google Cloud. To provide high quality service to our clients, we need to make use of additional tools though: Finance, Customer Support, Sales, Marketing and Development all need to use dedicated tools to work efficiently, and for this we need to share some data with those tools.

In order to guarantee the availability, integrity and confidentiality of data, this policy sets out requirements for employees of SI, which determine whether and how service providers can be commissioned with regard to maintaining confidentiality and data protection.

2. Scope of application

This policy applies to the commissioning of service providers by SI.

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information in the provision of services by service providers.

4. Principles of use of service providers

If service providers can gain access to company information and/or personal data processed by the company in connection with their work for SI, the assignment must be approved in advance by the superiors.

The superiors will contact the Data Protection and Information Security Team (DST) of SI in order to check and clarify the permissibility under data protection law and legal protection of the use of the service providers.

If it is not possible for the service providers to take note of personal data, a confidentiality agreement should nevertheless be concluded with the respective service providers. A template for such a declaration can be obtained from the DST.

All employees should note that in the event that service providers process data on behalf of the SI and/or maintenance or servicing of IT systems is carried out, during which it is theoretically possible to gain knowledge of personal data, it is mandatory to conclude a so-called Data Processing Agreement (DPA). Before the contract is concluded, the contractor must be inspected by the DST. For the information on new service providers, the form under the following link has to be filled out.

We share as little data as possible with the service provider, typically only admin names and email addresses. In cases when more transactional data has to be shared, like when SI needs to send an email about someone's performance review, the mail should still contain as little content as possible.

Furthermore, it is necessary to inform our customers should the service provider have access to customer data. In accordance with the agreed DPA with our customers, they have the right to object.

5. Sanctions

Violation of these guidelines may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

The contracts with the service providers should also provide for sanction options for violations by the service providers of the respective agreed duties in connection with data protection and information security.

Physical and Environmental Security Guideline

1. Introduction

Small Improvements Software GmbH (SI) Small Improvements has an office with workstations for the employees. In general, SI has no secret data within the office as all data is hosted on cloud servers. All devices are encrypted. Visitors are very rare and are always accompanied by employees.

2. Scope of application

This Physical and environmental security guideline applies to SI. They apply to all locations of SI.

These Physical and environmental security guidelines must be observed by all employees of SI.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

In order to guarantee the environmental security of the IT systems and personal data in the long term, the following rules must be observed by all employees.

4. Office Rules

The doors to the office are always to be kept closed so that visitors have to ring the bell to enter.

If there is no one in the office, it must be locked. The last person to leave the office is responsible for double-checking the doors.

As a digital company, SI does not have many printouts and paper. If it is necessary to print something, the paper should be shredded when it is no longer needed or kept locked away.

Each employee takes their laptop home. If this is not possible, the devices should be appropriately locked to avoid possible theft.

5. Visitors

Visitors are very rare and should always be supervised. Visitor management with badges or similar is not necessary.

As the doors are always locked, visitors must ring the bell to enter. Visitors are always asked who they would like to see and then escorted to the employee. If a staff member is expecting or has a visitor, the entire office is to be informed via the #berlin-office channel.

If you see unsupervised strangers in the office, ask them (in a friendly way) who they would like to meet and escort the visitor to the relevant employee.

6. Requirements for the design of the workplace

The workplace must be designed by employees in such a way that visitors or other third parties cannot gain access to personal data without being authorized to do so. For example, offices must always be locked after leaving the workplace.

When leaving the workplace PC, employees must “log out” or “lock” their PC so that authentication (username/password) is required before using the IT system and/or application(s) again.

The IT systems - especially the screens - must be set up in such a way that the risk of visitors or other third parties taking note is eliminated as far as possible.

In particular, in meeting rooms, connections to screens shall be disconnected during breaks and at the end of the meeting, and the presentation computer shall be locked.

Information in paper form must be filed in such a way that visitors or other third parties cannot gain knowledge of the data. Confidential information shall be kept under lock and key at all times.

7. Sanctions

A violation of these guidelines may constitute a breach of duty under the employment contract and be sanctioned accordingly.

IT Guideline for Employees

1. Introduction

Small Improvements Software GmbH (SI) has an IT infrastructure that is available to employees as a work tool in connection with their work for SI. The IT infrastructure is essential for the business operations of SI.

2. Scope of application

These IT guidelines apply to SI. They apply to all locations of SI.

These IT guidelines must be observed by all employees of SI.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

In order to guarantee the integrity, availability and confidentiality of the IT systems in the long term, the following IT guidelines must be observed by all employees.

4. General guidelines for the acceptable use of IT systems

Whenever the term IT systems is used in the following, it refers without exception to all devices or applications (hardware and software) with which information can be electronically processed or transmitted. This includes PCs, notebooks/laptops, tablet PCs (e.g. iPad), telephones, mobile phones, servers, storage media, network technology, software products and printers.

The use of IT systems and applications in the company is permitted exclusively for business purposes and to the extent permitted in each case for the performance of tasks. Deviations from this require the permission of superiors. Supervisors must agree on deviations with the company management.

Only software that has been approved by the company may be installed on IT systems of the company. Management may delegate this approval to IT officers and/or the Data Protection and Information Security Team (DST).

The use of private hardware and software for business purposes without authorisation is not permitted.

The use of IT systems at SI is basically for professional purposes only. Private use of IT systems of SI is generally prohibited, unless this or another company policy regulates exceptions to this or superiors have given express permission.

5. Compliance with legal regulations

When using the IT systems and applications at SI, employees must comply with the applicable legal provisions on data protection and data security as well as other legal provisions and company guidelines.

If employees are unsure whether and to what extent legal regulations or company policies must be complied with, they must contact their superiors for clarification.

6. Training

The company shall ensure that employees receive the necessary training and instructions required for their particular use of IT systems and/or applications.

7. General requirements for minimizing risks

In order to minimize the risks of data loss and IT emergencies, the following guidelines must always be followed:

- Data storage as well as the operation of business-relevant IT systems shall be carried out exclusively in the storage locations/areas specified in the Storage Locations Policy.
- When using external service providers, the “Guideline for Dealing with Service Providers” must be followed. The use of external service companies that either process data on behalf of SI or could obtain knowledge of data of SI must be coordinated with the DST

8. Guidelines for onboarding and offboarding

When onboarding a new employee, the Code of Conduct and the Confidentiality Agreement need to be signed, and all assets (especially the workstation) will be tracked in the asset list. All onboarding tasks are tracked via the templated onboarding Trello board.

Employees will get access to only those services containing customer data that they really need to access to perform their work, and they will only receive the permissions needed and applicable at that time. Once employees have proven themselves to be reliable and diligent coworkers their responsibilities will increase gradually, and so will their permission levels, but the “least privilege principle” (explained in more detail in the Authorisation Management Policy below) continues to apply.

Employees that leave on their own accord will typically hand in their resignation letters months or at least weeks in advance. We will adjust their work tasks so that they will not need far-reaching access levels in their final months and weeks anymore, and we will remove the corresponding permissions gradually. We will remove *all* system access on their last working day, so if they have remaining PTO they won’t have access on these days anymore. This includes email access. The only access left will be their Slack account, which will be turned into a single-channel guest account on their last working day, so they can still be reached in case of questions. In order to ensure no system is missed, final validation is performed by either the CTO or the CEO, who will double check all systems per our system overview list.

A stricter approach applies to employees who need to get terminated at short notice. In this case, all admin-level access has to be removed prior to communicating the termination, and all other access will be removed in the minutes right after the call.

All assets will have to be returned in time, and securely erased, and the asset list will be updated accordingly.

9. Guidelines for the use of passwords

As far as technically possible, all IT systems and applications can only be used after the user has been sufficiently authenticated. Authentication is usually done by using the username/password combination.

Security is paramount at SI, and using the right passwords is one core ingredient. Please observe the following requirements carefully:

- It's crucial that every employee uses **one-time passwords for every business service** they use on behalf of SI. Never use a password directly that you can remember, or (worse) that you've been using on another system. Instead, use a password manager such as 1Password (or the Apple Keychain) that will generate passwords, and store them. Choose a **strong master password** for 1Password and remember that one (and make sure you never use it anywhere else either)
- When setting passwords, **choose at least 14 random characters**, and unless the service prohibits this do include digits and special characters too
- Since we use one time passwords, we don't have to cycle passwords. If one service we use was compromised, change that password, but there's no need to change anything else.
- **Multi-Factor** authentication should be used whenever possible. It *must* be used on all systems that enable access to confidential data (like customer data), and it must also be used systems where your access level could be exploited to cause harm (if you have edit rights to the website for instance : the website has no customer data, but installing malware on the website would of course be disastrous still)
- **Do not share personal passwords!** The only possible exception is if we use a service that simply doesn't allow multi-user access, like Instagram for instance. In that case, create a secure "vault" in 1Password and share the password only with the people who absolutely need access. Change the password once a person doesn't require access anymore (or is leaving the company)
- **Change initial passwords immediately:** In some cases we will set up a new account on behalf of staff and we *have* to assign an initial password. Most systems require the new employee to change the password immediately. In case the system does not mandate this, it's on the employee to set a new secure password.

- **If in doubt, change your password!** If a service you use has been compromised, or *may* have been compromised, immediately change your password.

10. Protection against malicious content

It's crucial our computers are not getting infected with malware, since that would bypass *any* of our other security measures.

To achieve this, several measures are required

- The biggest threat to an already security-conscious organization like Small Improvements is malware that disguises itself as useful software. Any small useful utility (like a timezone conversion tool, or audio-player) can turn out to be spying on the user, or – even if not harmful today – get hacked eventually and turn into Malware. Therefore employees are requested to install software from trusted vendors only, from vendors that have been pre-approved by the company, or approved on the spot by their team's Team Lead. The goal is to minimize potential attack vectors, so employees are not allowed to install software on work computers unless it's required to do the job, and unless they know a software has approval from the company. Employees may always request access to new software of course, but the company needs to know and approve.
- Another key attack vector is malware sent by mail: Everyone is required to be very skeptical at any unsolicited mail, and at any odd-sounding mail that requires to open attachments of click links. Even coworkers' mails need to be viewed with scrutiny to avoid falling victim to a coworker who has been hacked and starts sending malware mails
- Further Malware attack vectors are dodgy or breached websites. Only use up-to-date browsers that are considered safe, like Chrome, Safari, Firefox, or Edge, and avoid sites that are neither work-related nor informational
- Firewalls: Every employee is required to enable their operating system's firewall and keep it enabled
- Antivirus: Any computer with an operating system prone to viruses (essentially meaning all Windows computers) need to run up-to-date Antivirus software. The company will make recommendations as to what software to use. Apple and Linux computers are exempt from this policy since viruses are effectively prevented by the operating system, and no antivirus software provides better support than the built-in mechanisms.
- Operating system updates: Every employee is required to keep updating the operating system at all times. This is usually easy since the OS prompts the user, but one still has to accept the update, and everyone is required to do so whenever feasible.

11. Pre Approved installable tools

This is a non-exhaustive list of pre-approved software. We update this list frequently internally, but don't necessarily update it in this guideline immediately. We merely provide it as an indication of how we work.

- Adobe Products
- Apple Products
- Microsoft Products
- Google Products
- Design tools: Sketch, Figma, Skitch
- Dev Tools: Jetbrains & Github products, JProfiler, Emacs, vim, and comparable popular and trusted dev tools
- Mail: Thunderbird, Evolution
- Browsers: Chrome, Firefox, Opera
- Productivity: Slack, Zoom, Goto-Meeting
- Music: VLC Player, Spotify, Soundcloud

12. Guideline on the use of e-mail/internet

Employees shall be provided with a business email account. Email may only be used for business purposes.

Employees may be permitted to receive and send private email through their own private webmail account. The extent of this use may be restricted by the company for operational reasons.

Email is by default not a secure communications mechanism. Emails are transmitted in plaintext, and there is no guarantee that the person pretending to send a mail is actually that person, nor that your mail will reach the right person. A lot of our communication has moved from email to internal tools like Slack, Trello or Confluence – but even so, email remains a common part of our work lives, and there are risks associated with every attachment, every link, and any information (and which may or may not be true.).

To make the use of email as safe as possible, the following rules must be observed.

- When reading or sending mail, employees should always consider the worst. It could be that it’s not a coworker sending an interesting file, but actually an adversary who wants you to install some malware, or get confidential information out via social engineering. If in doubt, employees should always double check in person, via phone, or at least via Slack.
- No sharing of confidential information via unencrypted mail. Either an encryption is set up, or merely mail is used as a notifying mechanism for data that was sent some other way.
- Do not encrypt a file and then send a second mail that contains the password.
- When possible, using mail should be avoided and internal tools should be used like Slack for direct or group communication, and Confluence for bigger topics and company-wide discussions. The risk of someone *pretending* to be the manager or a coworker on Slack is much smaller than in mail, and the risk of someone spying is smaller. (Naturally, even notes and information shared via these systems have to be treated carefully. A coworkers’s Slack account may have been compromised.
- When possible, even employees should invite external partners into a shared Slack channel, rather than sending information via mail.

- Sometimes customers want to send data. Employees should encourage them to use more secure systems than sending mail. Customers shouldn’t send their employee data via unencrypted mail to SI.

If employees become aware that the protection or security of data may be compromised in any way, they must immediately contact the DST and their supervisors. This applies in particular if the threat relates to personal data.

13. Definition of emergency and emergency plan

An emergency can jeopardize business operations in the long term.

If emergencies occur that affect the functioning of the IT systems, an emergency plan is applied.

The emergency plan defines an emergency definition, a specification of the persons responsible, the notifications as well as the emergency measures.

In the event of an emergency, the guidelines of the emergency plan apply with the purpose of maintaining business operations or immediately restoring a state of functioning IT infrastructure.

The emergency plan is regulated in a separate document and describes these points.

14. Logging

Various information is logged in the IT infrastructure in order to be able to quickly identify and remedy malfunctions, failures and security incidents. In doing so, the relevant data protection regulations are observed and the personal rights of employees are protected.

During regular operation of the IT infrastructure, connection data (date, time, addresses of sender and recipient, the type of data transferred, the volume of data transferred, etc.) is logged by various systems (especially applications, servers and firewalls). In the course of using the IT infrastructure, data is logged from which user behavior can also be traced in whole or in part (time of logging on and off IT systems, date and time of changes in files, etc.).

To meet legal requirements, the company archives all incoming and outgoing emails at least for the duration of legal retention obligations. These can be up to ten years. For certain data, longer retention periods may also apply.

The collection of this log data is necessary for the secure and legally compliant operation of the IT infrastructure.

The log data is used exclusively for the following purposes:

- Analysis and correction of malfunctions, failures and security incidents.
- Ensuring the security of the IT infrastructure

- optimisation of the IT infrastructure
- for statistics on the use of the IT infrastructure and for
- non-personal random checks and evaluations in accordance with this policy (see section “Abuse Control”).

The log data will not be used for performance and behavioral control of employees.

15. Misuse control

A non-personal evaluation of the log data is carried out by specially commissioned employees to identify malfunctions, failures and security incidents.

A personal evaluation of the log data only takes place if there is a concrete suspicion of misuse, unauthorized or punishable use of the IT infrastructure on the basis of a spot check, a report or other suspicious facts.

In this case, the following procedure is binding:

- A personal review of the log data is only carried out in the case of a weighty suspicion of misuse; petty cases do not justify the review.
- The review is carried out according to the principle of data economy.
- It is carried out with the mandatory participation of the data protection commissioner.
- If the suspicion is not confirmed by the review, the data and records collected for the review shall be deleted immediately. The unconfirmed suspicion must not lead to any further follow-up measures - in particular no targeted spot checks against the employees concerned.
- In case of imminent danger, SI will immediately prevent further endangering or punishable actions - possibly by involving the criminal prosecution authorities. In particular, the necessary technical defense measures will be taken without delay, even if personal data have to be collected or viewed in the process. The DST shall be informed immediately of the events.

16. Sanctions

A violation of these guidelines may constitute a breach of duty under the employment contract and be sanctioned accordingly.

Authorisation Management Policy

1. Introduction

At Small Improvements Software GmbH (SI), various applications are used on different IT systems.

We manage highly confidential customer data, our own financial data, and plenty of our business plans and goals. The moment adversaries get access to this data, our entire business is at stake. We need to ensure that we only use systems we trust, and that we only give access to staff we trust.

In addition though, it's important to remember that even a person we trust may have their account breached by intruders. So even the most trustworthy staff member should only get access to just as much data and applications that they can do their job well, and also only for the time they need and but not longer ("least privilege principle")

2. Scope of application

This guideline applies to all locations of SI. It obliges all employees of SI to adhere to the specifications set out here.

In the following, employees are uniformly referred to as "employees". For reasons of better readability, the generic masculine is used. Female and other gender identities are expressly included.

3. Guidelines for authorisation management

3.1 Basic requirements for the management of authorisations

Before any IT resource is put into operation, a "responsible person" must be appointed for the IT system or application. The responsible person determines, in consultation with the Information Security Team, the extent to which users should be able to access the IT resource.

In this context, permissions for different types of users ("users") should be grouped into "user roles/groups" in order to be able to assign the appropriate role to individual users when setting up access.

3.2 Regulation for setting up users and user groups

A separate administrative role must be set up for each IT resource and assigned to the persons administering the IT resource.

New user groups may only be set up by the Information Security Team with the involvement of the respective person responsible for the IT resource. When setting up user groups, the principle of necessity and actual need shall be taken into account.

New users may only be set up according to the “dual control principle”. A user is set up by an administrator of the respective IT resource if the following requirements are met:

1. The person responsible for the IT resource requests the creation of a user from the Information Security Team in text form (e.g. via a ticket system), stating the name and, if applicable, further contact details as well as the user to which the new user is to be assigned.
2. The responsible person will apply the so-called “least privilege” principle to the request. According to this, users are only to be assigned the rights that are actually required for the assigned tasks in the company.
3. If a user is to be given more rights than those of the assigned user group, these are to be defined and justified by the Information Security Team with the management. The same applies to a “less” of permissions.

Furthermore the following principles have to be observed:

- Employees should never share any crucial passwords between staff. Only use and commission new systems that support multiple user accounts.
- 2-factor authentication has to be enabled, when dealing with important data, especially if the employee is an admin, but also when possible as a normal user.
- The main admin accounts are assigned by the CTO by the Information Security Team. For each system there are also system-owners who are in charge of assigning new users when needed.
- If API keys must be used to access another application from SI, these API keys must be treated like a password and must not be shared. They should be stored in 1Password and only given to those who really need them.
- Administrators of any system must ensure that they only grant additional access (both in terms of new users and additional privileges) on a strict need-to-know basis. Check with the system owner, or with the Information Security Team (or with the CTO) if in doubt.
- Always consider giving permissions on a temporary basis. Perhaps someone only needs access for a week. Temporary permissions should be revoked once the task is completed.

3.3 Documentation of user groups and authorisations

The person administering an IT resource is obliged to document the creation, modification and withdrawal of authorisations. The same applies to user groups. The documentation shall be protected from unauthorized access. The availability and integrity of the documentation must be guaranteed.

3.4 Regulation for the modification and withdrawal of authorisations

In the event of personnel changes of users, the authorisations shall be adjusted by the Information Security Team.

The Information Security Team routinely revisits all systems and removes people who don’t require access anymore. If in doubt, we’ll err on the safe side. So if your account was downsized or removed by accident, please let them know, it was not done with bad intentions, we’ll reinstall your permissions so you can do your job.

3.5 Regulation of password use

The password specifications include a minimum password length of 14 characters, whereby the password must consist of upper/lower case letters, numbers and special characters.

There is no provision for changing passwords. If systems or applications provide for a password change, this is only permitted in justified cases.

A password history is stored as far as possible. This ensures that the past ten passwords cannot be used again.

The persons administering an IT resource are obliged to use secure procedures for assigning new passwords to users when resetting passwords. The aim is to ensure that unauthorized persons do not gain access to IT resources through a password reset.

Unauthorized attempts to access IT resources shall be restricted in such a way that in the event of multiple accesses with incorrect access data, a (temporary) blocking of the respective account is carried out.

4. Sanctions

A breach of this policy may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

Guideline for the use of mobile data carriers

1. Introduction

At Small Improvements Software GmbH (SI), mobile data carriers may be used in some cases.

This guideline regulates the use of mobile data carriers by employees of SI.

2. Scope of application

This guideline applies to the use of mobile data carriers of SI. Mobile data carriers are all easily transportable devices on which data can be stored. This includes in particular USB sticks, external hard drives, memory cards, CD-ROMs and DVDs.

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information on mobile data media.

4. Principles of the use of mobile data carriers

Mobile data carriers bear the risk that unauthorized third parties may come into possession of information of SI or customers and/or business partners of SI.

Therefore, mobile data carriers are only to be used by employees who are dependent on the use of mobile data carriers due to their work at SI.

Data on the mobile data carriers must always be stored in encrypted form if they represent personal data and/or may contain company and business secrets of SI or third parties.

When implementing encryption, users must ensure that an encryption method is used which has been approved by the IT department of SI.

The unencrypted storage of the above data is only permitted in exceptional cases. It must be approved by superiors in text form (e.g. e-mail).

Data on mobile data carriers, if these are intended for permanent storage at SI, are to be transferred immediately to the storage drives of SI intended for this purpose, if they are not already available there. When transferring the data, special care must be taken to ensure that the contents on the data carrier are checked for malware. The employees concerned must also ensure that it is possible for SI to decrypt the data at any time.

You can contact the Information Security Team if they have any questions regarding implementation.

You may not allow other persons to use the mobile IT system made available to them.

With regard to the installation of software on the mobile IT systems, the “IT Guideline for Users” applies.

5. Use of mobile data carriers outside the company

If mobile IT data carriers are used outside the premises of SI, the users must take special care to ensure that third parties cannot obtain knowledge of information. This includes, in particular, the careful and secure storage of the mobile data carrier in order to protect it from theft and loss.

6. Mobile data carriers from third parties

Should you find a mobile data carrier on the company premises or elsewhere, such data carriers must never be connected to IT systems of SI. It cannot be ruled out that the data carrier contains malware or spyware. Found data carriers must be reported to the Information Security Team and carefully inspected by them with regard to harmful contents or destroyed.

The same applies to data carriers that have been handed over to employees by third parties.

7. Theft and loss

If a mobile data carrier is stolen or lost, the employees concerned must report this to the Data Protection and Information Security Team (DST) immediately after becoming aware of it.

The report must be made as soon as possible, as in these cases there may be legal obligations to provide information to supervisory authorities and data subjects, which may result in fines of a considerable amount if the report is made too late.

The notification can be made by e-mail to the known e-mail address of the DST.

8. Sanctions

A breach of these guidelines may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

Guideline for the use of mobile IT systems

1. Introduction

Small Improvements Software GmbH (SI) has an IT infrastructure that is available to employees as work equipment in connection with their work for SI.

Mobile IT systems are also in use at SI. In order to take into account the special risks arising from the use of mobile IT systems, the use of these systems is regulated separately by this guideline.

2. Scope of application

This policy applies to the use of mobile IT systems of SI.

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information on mobile IT systems.

4. Principles of the use of mobile IT systems

Mobile IT systems bear the risk that unauthorized third parties can come into possession of information of SI or customers and/or business partners of SI.

Therefore, mobile IT systems are only to be used by employees who are dependent on the use of a mobile IT system due to their work at SI.

In principle, data is only to be stored on mobile IT systems if this is necessary for the fulfillment of the employees’ tasks in connection with their work for SI or for purposes of SI.

As far as technically possible, data on the mobile IT systems shall be stored in encrypted form. When implementing the encryption, employees must ensure that it is possible for SI to decrypt the data at any time. Employees can also contact the IT department in this respect if they have any questions regarding the implementation.

Employees may not leave the mobile IT systems made available to them to other persons for use.

With regard to the installation of software on the mobile IT systems, the “IT Guideline for Users” applies.

5. Use of mobile IT systems outside the company

If mobile IT systems are used outside the company premises of SI, the employees concerned must take special care to ensure that third parties cannot obtain knowledge of information that is processed with the mobile IT system.

If possible, information requiring special protection should only be processed at locations that cannot be viewed by third parties.

If this is not possible, employees must choose a location or place for processing data that ensures that the screen cannot be viewed by third parties. If possible, the mobile IT system should be equipped with privacy devices (e.g. privacy film for notebooks).

6. Data Backups

Users of mobile IT systems must ensure that data which is stored locally on the device is transferred at the earliest opportunity to data storage devices which SI normally uses for storing company data.

If there are any questions about the procedure for transferring the data, the employees concerned must contact the Information Security Team.

7. Theft and loss

If a mobile IT system is stolen or lost, employees must report this to the Data Protection and Information Security Team (DST) and to the management immediately after becoming aware of it.

The report must be made as soon as possible, as in these cases there may be legal obligations to provide information to supervisory authorities and data subjects, which may result in significant fines if the report is made too late.

The notification can be made by e-mail to the known e-mail address of the DST.

8. Sanctions

A breach of these guidelines may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

Policy for storage locations

1. Introduction

At Small Improvements Software GmbH (SI), data can be stored on various IT systems (“storage locations”).
In order to ensure the availability, integrity and confidentiality of data, this policy sets out requirements for employees of SI as to where data is to be stored.

2. Scope of application

This policy applies to the storage of data in connection with work for SI.

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine form is used. Female and other gender identities are expressly included.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information by specifying storage locations.

4. Principles of data storage

As a matter of principle, data should not be stored on local hard disks or data storage devices of end devices. In addition to the lack of availability of the data, the main reason for this is that in these cases it is not possible to adequately guarantee the security of the data.

The storage of data must always take place in the directories/folders of servers or IT systems that are released for the respective employees.

If it is not possible to assign data to a specific department, group or project folder, the data must first be stored on the employee’s own “home drive”. Otherwise, data must always be stored in the relevant department, group or project folders.

When using mobile IT systems and mobile data carriers, the applicable guidelines must be observed.

5. Data Encryption

All data is encrypted during transit using HTTPS/SSL. Furthermore all data is encrypted by default in the Google Data centers, by Google. In addition,the string-based content is encrypted such as the written feedback, objectives, performance reviews in the database on a per-field basis, using symmetric AES-256 encryption, making it even harder to analyze the data in case of a database breach.The encryption/decryption process happens on the server, at the so-called service level, before and after accessing the database. A different key is used for each customer, which makes the logical separation of the data even clearer.

Customer data is stored logically separated from each other in the databases, and only pseudonymized or anonymized data will be used for test purposes. Development and QA environments are entirely separated from the production database.

6. Data backup

SI shall agree with its administrators which data is to be backed up, at what frequency and on which media or at which locations. The data backup strategy must be documented by the responsible administrators.

Data backups must be made at least daily. In addition, a weekly full backup and a monthly full backup must also be made.

Requirements

- daily snapshots of all production data stored on an independent system.
- Notification in case a backup didn’t succeed
- Replaying of backups frequently in order to ensure they are still working
- Deletion of backups after 6 months

Implementation

- The Application runs in Google Cloud App Engine, the live database being in Google Data Store. The backups are stored in the Google Cloud Storage service, which is entirely independent. Even if a coding error or App Engine related problem led to the entire database being wiped, we’d be able to recreate the database within hours.
- A daily notification email is sent to key staff when a backup has been created. If any part of the process has failed, this is clearly stated in the subject line of the email and immediate action is taken to ensure that the backup works.
- At least every 2 months, a backup copy is taken and played to an empty server to ensure that the process is still working.
- Backups are deleted after 6 months

Replication

- It is important that there is no single point of failure. All production systems must survive the failure of individual servers or even entire data centers.

7. Data retention

SI shall retain customer data for as long as an organization remains a customer. Once the contract expires, data shall be securely erased after 30 days the earliest. Customers are given notice so that they can download the data they wish to retain.

Customers may decide at their own discretion to delete data before the contract expires, either by deleting parts of their content, or by erasing all of it.

Customer data that is deleted from the database will still continue to exist in backups for 6 months, until the backup gets deleted after 6 months. Contract data like invoices will be retained for 10 years in SI’s German office due to legal and tax reasons.

8. Regulations for administrators

Administrators are obliged to document all storage locations provided for SI and to include them in a directory with the respective purpose of the directory. If necessary, the required authorisations (groups/roles) must also be stored in the directory.

If new storage structures are created by administrators, this must be agreed with the company management.

9. Sanctions

Violation of these guidelines may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

Security Incident Policy

1. Introduction

This policy governs the handling of security incidents at Small Improvements Software GmbH (SI).

2. Scope of application

This policy applies to the entire IT infrastructure of SI.

This policy applies to all locations of SI.

This policy obliges all employees of SI SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine is used. Female and other gender identities are expressly included.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information of the IT infrastructure of SI.

4. Principles

The IT infrastructure of SI includes, without exception, all devices and applications that process, transmit or store information electronically, such as workstation PCs, servers, printers, storage media, telephones, fax machines, mobile phones, smartphones, tablet PCs and the like.

A security incident is an undesired event that has an impact on information security and/or the protection of personal data and can result in major damage.

Employees are hereinafter uniformly referred to as “staff members”. For better readability, the generic masculine form is used. Female and other gender identities are explicitly included.

5. Notification

Security incidents can have significant, negative consequences for the company. Even if a security incident is suspected, a report must be made immediately by the employees who notice the security incident.

The only exceptions to this are if the employees in question know for certain that the security incident has already been reported by other employees. In case of doubt, a report must be made.

Security incidents have the highest priority. This means that the reporting of security incidents always takes precedence over day-to-day business or other current work.

If in doubt, classify the security incident with a high severity level. The incident is to be posted immediately in Slack with #incidents. A downgrade and all-clear is possible at any time.

6. Handling of the security incident

6.1 Classification

High

There are indications or reports that data or security or privacy has been breached or that a vulnerability or defect threatens security - e.g. hackers can access data, companies or users see data they should not see, etc.

Stays high, when it has been confirmed, that the incident is indeed possible.

Priority: Immediate reaction, everything else is to be dropped

Medium

We have identified that the issue is not exploitable or not in our system, or that a user error/UX issue is at play.

Priority: Can be dealt with the next day and will either be moved to a follow-up ticket (bugs or technical roadmap) if the risk assessment justifies it, or closed (in case of false alarm).

6.2 Steps

Step 1: Ring the alarm

- Everyone is to be informed immediately in the Slack channel **#incidents**. In particular, the data protection and information security team (DST) and the CTO are to be informed.
- A conference call is to be held as soon as possible.
- The following details are to described:
    - Severity
    - All known details
    - Who reported the incident and when, through which channel.
    - Scope (type and amount of data potentially compromised, globally or for a single customer...)

    - Identification of the owner of the incident and the members of the team responding to the incident
    - Clarification expectations for response time

If there is evidence of a data breach or major security incident, the Data Protection Officer helps to determine whether the incident needs to be reported to the authorities
or not. For this purpose, the Data Protection Officer shall conduct a risk analysis in the data protection management system.

When in doubt, it is better to involve more people, it is efficiency and speed that matters most.

Step 2: Fix & preserve

- The affected systems must be shut down if there is a suspicion that there has been a data or security breach that can be further exploited
- If a customer account is particularly affected and data may be leaking out, it must be locked.
- All forensic evidence of the breach shall be preserved if external influences are present
    - Google request logs with a timestamp and IP address
    - Internal log messages
    - audit records
- Analyze whether this issue could affect and endanger neighboring systems
- Investigate root cause and fix the problem

Step 3: Document & inform

- Documentation of the incident thoroughly
- If data has been leaked or security has been breached,
    - Customer-Team: notify affected or at risk customers within 8h with details on the scope of (potential) breach, an update on the situation, and a timeline when to expect the next update
        - using email and consider in-app messages
    - information to our Data Protection Officer
    - documentation of every step
- if applicable (e.g there is a security breach on premises) notify law enforcement agencies

Step 4: Post-mortem

- Run a thorough post-mortem with actions to prevent this type of incident in the future.

7. Sanctions

A breach of these guidelines may constitute a breach of duty under the employment contract and may be sanctioned accordingly.

Guideline for dealing with malfunctions and failures

1. Introduction

This policy regulates the handling of malfunctions and failures of IT systems at Small Improvements Software GmbH (SI).

2. Scope of application

This policy applies to the entire IT infrastructure of SI.

This policy applies to all locations of SI.

This policy obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”.

3. Objectives

This policy is intended to help ensure the integrity, availability and confidentiality of information of the IT infrastructure of SI.

4. Principles

The **IT infrastructure** of SI includes, without exception, all devices that process, transmit or store information electronically, such as workstation PCs, servers, printers, storage media, telephones, fax machines, mobile telephones, smartphones, tablet PCs and the like.

A **disruption** is a situation in which processes or resources of SI do not function as intended and the resulting damage is to be classified as minor. In principle, a minor disruption exists if the removal of the disruption can be carried out in the general course of day-to-day business.

A **failure** exists if a part or parts of the IT infrastructure have lost their ability to function.

5. Notification

Malfunctions and failures impair the company’s ability to function and can lead to costs and further damage. If faults and failures are not reported or are reported too late, this can lead to consequential damage, which must be avoided.

In order to be able to quickly remedy malfunctions and failures, immediate reporting of corresponding incidents is necessary.

All employees must report possible malfunctions and failures to an **administrator**. If they are not available, the report will be made to the supervisors. They will forward the report to an administrator or the management.

In the case of serious failures, employees must also inform the management immediately. A failure is considered serious if one of the following characteristics applies:

- Injury to life or limb
- Failure of financial accounting
- Failure of order processing
- There is a violation of laws, contracts or standards and liability risks have arisen which are considerable for the company or for individual responsible persons, in particular possible violations in the area of data protection.

6. Sanctions

A breach of these guidelines may constitute a breach of duty under the employment contract and be sanctioned accordingly.

Emergency plan

1. Introduction

This emergency plan regulates the handling of emergencies at Small Improvements Software GmbH (SI).

2. Scope of application

This emergency plan applies to the entire IT infrastructure of SI.

This emergency plan applies to all locations of SI.

This emergency plan obliges all employees of SI to comply with the duties and requirements set out herein.

In the following, employees are uniformly referred to as “employees”. For reasons of better readability, the generic masculine is used. Female and other gender identities are expressly included.

3. Objectives

This emergency plan is intended to help ensure that the integrity, availability and confidentiality of information of the IT infrastructure of SI is guaranteed or can be restored as quickly as possible.

4. Definition of emergency

An emergency is an undesired, temporally unforeseeable event that can endanger business operations in the long term. In the event of an emergency, the following guidelines apply with the purpose of maintaining business operations or immediately restoring a state of functioning IT infrastructure.

5. General behavior

In the event of an emergency, a prudent approach is particularly necessary. The priority in an emergency is to remain calm. The situation must be analyzed immediately and the reporting plan must be adhered to.

In the event of a mere suspicion of irregularities indicating an emergency or impending emergency, superiors and the Data Protection and Information Security Team (DST) must always be informed.

6. Fire

In the event of a fire, the fire brigade must be informed immediately.

Furthermore, the supervisor, the management and the DST are to be informed immediately.

In the event of a major fire incident, the employees at the respective premises shall be evacuated immediately. Escape route plans are posted in a conspicuous place in the building.

7 . Water

Major water damage that could negatively affect the critical IT systems required for business operations poses only a very low risk at all operating sites due to their location.

It is not regularly expected that water damage will lead to an impairment of the critical IT systems. The IT systems are located in places where there is no risk of flooding. Damage caused by water pipes is also extremely unlikely due to the spatial conditions.

Should water damage nevertheless occur that could pose a risk to the critical IT systems or other IT systems, the supervisor, the DST and the IT department must be informed immediately. They will then carry out a risk assessment and further necessary measures after reviewing the situation.

8. Power failure

All critical IT systems that are essential for business operations have an uninterruptible power supply (UPS). This ensures that power outages of several minutes can be bridged and that in the event of a prolonged power outage, the IT systems can be shut down in an orderly manner to ensure the integrity of the data.

The essential part of the critical IT systems is located in a data center that has generators with alternative power generation in case of a power failure, thus ensuring availability of the IT systems even in case of prolonged power failures.

9. Failure of IT systems

All critical IT systems are subject to monitoring, which is used to monitor availability and any failures.

In the event of a failure, the IT staff member on duty is automatically informed. He or she will immediately check the incident and, in the event of more than brief, temporary disruptions, inform superiors without delay.

The reason for the failure must be remedied immediately. In the case of critical IT systems, care must be taken to ensure that sufficient spare parts and/or replacement systems are always available to bridge or eliminate the failure at short notice.

1. External attacks: All server IT systems and all critical IT systems are secured and monitored by firewall technology. This makes it much more difficult for unauthorized third parties to gain access from the outside. The firewall technology is regularly maintained and updated to ensure adaptation to new threat situations.
2. Break-in and theft: All office and business premises are secured against access by unauthorized third parties. This applies in particular to access to the building outside office and business hours.

All critical IT systems are located in specially secured premises (e.g. data centers) which can only be entered after appropriate authentication.

In the event that a break-in and/or theft of IT systems is detected, the respective employees must immediately inform their superiors, the DST and the management.

1. Failure of IT administrators: Only a few people in the company have administrator rights. These persons are appropriately trained and educated. In the event of a failure of IT administrators (e.g. due to illness), care has been taken to ensure that at least one other person with administrator rights is immediately available to carry out any necessary administrative actions.
2. Person responsible for emergencies: There is an emergency officer in the company who is responsible for initiating the respective planned and required measures in the event of an emergency.

This is a person appointed by the management. If this person is not available, the management must be contacted.

10. Recovery plan

The Information Security Team shall ensure that the necessary backups and backup systems are always available for critical IT systems and that recovery plans are in place.

The recovery plans shall in any case also be documented and available in a place that is quickly accessible even in the event of an emergency and ensures that the actions indicated in the recovery plans can be started immediately.

In the event of a functional failure of an IT system, the cause of the incident is immediately investigated. Parallel to this, measures are immediately initiated to enable the IT system or a backup system to be restarted at short notice.

In the IT department, all responsible persons are trained to investigate a functional failure and to restart the critical IT systems as quickly as possible. Special care must be taken to ensure that the integrity of the data is guaranteed.

11. Address list / message list

Here you will find an overview of the persons responsible for the areas mentioned:

Per Fragemann, CEO, per@small-improvements.com
Berit Schubert, DPO, b.schubert@ds-lud.de
Peter Crona, CTO, pcrona@small-improvements.com