GTC + SLA

General Terms and Conditions SoSafe GmbH

Version 18.08.2021

Section A -- General Provisions

1. Nature and scope of these GTC

1.1 SoSafe GmbH, Ehrenfeldgürtel 76, 50823 Cologne, Germany (hereinafter referred to as **"SoSafe"**) offers the implementation of comprehensive awareness building in the field of cyber security (hereinafter referred to as **"Awareness Building"**) for companies, public authorities and other organizations (hereinafter referred to as **"Customers"**).

1.2 These General Terms and Conditions (hereinafter referred to as **"GTC"**) as well as the Service Level Agreement (**"SLA"**), attached as **Annex 1**, are an integral part of the Awareness Building Agreement between SoSafe and the customer and are valid for all customers. In addition to the provisions in this Part A of the GTC, the provisions in Part B of these GTC shall apply to the use of web-based services. As far as in the following paragraphs of these GTC are referred to without any special mention of part A or B, the paragraphs of the same part from which the reference is made are meant.

1.3 Awareness building consists of four different modules (hereinafter referred to as **"service modules"),** some of which are supplemented by other services and software tools. These include (i) phishing simulations, the provision of (ii) e-learning modules based on them, a (iii) phishing notification button and the (iv) SoSafe Manager. Some of the service modules are made available web-based via the SoSafe platform (hereinafter referred to as **"Platform"**) at https://elearning.sosafe.de (for access to the E-Learning modules) or at https://manager.sosafe.de (for access to the admin and reporting dashboard).

1.4 SoSafe offers the service modules in different service packages defined in the SLA (hereinafter **"service package"**). Depending on the service package, the service modules are provided to the customer to a different extent (number of users, number of accessible modules etc.) and with different additional services. If the contract is concluded via the website operated by SoSafe (https://app.sosafe.de/) the customer can only order the service package "Starter".

1.5 The version of these General Terms and Conditions that is valid at the time of the conclusion of the Awareness Building Agreement is applicable.

1.6 The validity of general contractual or business terms and conditions of the customer is expressly excluded. This shall also apply if SoSafe has not expressly contradicted the conditions of the customer. Separate, bilaterally agreed upon appointments remain unaffected.

1.7 The GTC of SoSafe are only valid for companies in the sense of § 14 BGB (German Civil Code), legal entities under public law and special funds under public law.

2. Contracting and scope of services

2.1 The Awareness Building Agreement, if offered, can be concluded either via the website https://app.sosafe.de/ operated by SoSafe or offline by accepting an offer of the customer.

2.2 If the Awareness Building Agreement is concluded offline, it shall be concluded if SoSafe accepts the order or the assignment of the customer (offer of the customer) within 7 calendar days after receipt. The acceptance, signed copy of the order/contract can be made either by mail or in electronic form.

2.3 All documents sent to the customer concerning possible services and prices of SoSafe with regard to the envisaged Awareness Building Agreement are subject to confirmation and non-binding, unless they are explicitly marked as a binding offer or contain a certain period of acceptance.

2.4. As far as the Awareness Building Agreement is concluded via the website operated by SoSafe, the Awareness Building Agreement can be concluded in German language and will be concluded via the following technical steps:

- The awareness building services offered on the SoSafe website do not constitute a binding offer to conclude a contract. It is rather an invitation to the customer to submit a binding offer.
- By clicking the order button, which is marked "Buy annual licenses", the customer submits his binding offer.
- SoSafe shall confirm to the customer the receipt of his declaration of offer by electronic means to the e-mail address indicated by the customer immediately after its submission. This declaration of receipt shall not constitute an acceptance of the customer's offer.
- The binding acceptance of the offer of the customer by SoSafe shall be effected by sending a separate explicit declaration of acceptance by e-mail.
- During the term of the Awareness Building Agreement the customer shall be able to view the details of his contract with SoSafe via his account at any time.

3. Contract period and termination

3.1. The Awareness Building Agreement on which these GTCs are based is concluded for the agreed period. The period of the contractually agreed Awareness Building services shall commence at the time the service is provided to the customer, but no later than 30 days after the conclusion of the contract. After expiry of the agreed period or at the end of the contract after termination, the Awareness Building services will no longer be provided and the customer's access rights to the platform will be blocked.

3.2. Both the customer and SoSafe shall have the right to terminate the agreement on Awareness Building for good cause without observing a period of notice. An Good cause is in particular for SoSafe:

- a serious breach by the respective customer of the provisions of these GTC, including the SLA, or
- the opening of insolvency proceedings against the assets of a customer or the rejection of the corresponding application to open insolvency proceedings for lack of assets.

3.3 Any termination must be in writing. Termination by e-mail is also permissible.

3.4 The Awareness Building Agreement shall be extended by one (1) additional year if the Awareness Building Agreement is not terminated by either party one (1) month before the end of the respective contract period.

4. Terms of payment

4.1 The payment is based on the individual contract with the customer. Differently, if the conclusion of the contract, as described in clause 2.4., has been made via the website operated by SoSafe: In this case the payment shall be displayed before sending the offer declaration, depending on the number of ordered licenses. All payments agreed upon in the Awareness Building Agreement are net amounts and are subject to VAT at the statutory rate.

4.2 Unless otherwise agreed upon, SoSafe shall issue an invoice immediately after the conclusion of the contract for the entire agreed term of the contract. This shall also apply to multi-year licenses. In this case, the services for the entire performance period shall be invoiced upon conclusion of the contract, unless otherwise agreed. In case of a contract extension, the invoice will be issued in full at the beginning of the respective extension period. All invoices of SoSafe are due within 14 calendar days and payable without deduction.

4.3 If after the conclusion of the contract a significant deterioration of the financial circumstances of the customer occurs, SoSafe shall be entitled to demand advance payments or security within a reasonable period of time and to refuse performance until the contract is fulfilled. In case of refusal of the customer or fruitless expiration of the deadline SoSafe shall be entitled to withdraw from the contract or to claim damages for non-performance.

4.4 A payment shall only be deemed to have been made when SoSafe has the full amount at its disposal. In case of cheques, bank transfers or card payments the payment shall only be deemed to have been made when the amount has been finally credited to the account of SoSafe.

5. Further development of our services, handover

5.1 SoSafe reserves the right to extend, supplement or change individually offered services at any time, as long as this leads to an improvement of the service for the customer or does not or does not significantly affect it.

5.2 SoSafe shall make the platform, including the services to be provided through it, available on servers for use at the access point of the data processing center of SoSafe ("transfer point of the service"). In order to use the platform it is necessary that the client has his own access to the Internet and that he uses this access to access the platform at the transfer point of the service.

6. Liability, limitation of liability

6.1 SoSafe shall have unlimited liability for damages resulting from injury to life, body or health, which are based on a breach of duty by SoSafe, a legal representative or vicarious agent of SoSafe, as well as for damages caused by the absence of a quality guaranteed by SoSafe or in case of fraudulent conduct by SoSafe.

6.2. SoSafe shall be liable without limitation for damages caused by SoSafe or a legal representative or vicarious agent of SoSafe intentionally or by gross negligence.

6.3. In case of a breach of essential contractual obligations caused by slight negligence SoSafe shall only be liable to the extent of the typically foreseeable damage, except in the cases of clause 6.1. or clause 6.2.. Essential contractual obligations are abstractly such obligations, the fulfillment of which makes the proper execution of an agreement possible in the first place and on the compliance with which the contracting parties may regularly rely.

6.4 Liability under the Product Liability Act remains unaffected.

6.5 Any further liability of SoSafe is excluded.

6.6 The limitation period for claims for damages of the customer against SoSafe shall be one (1) year, except in the cases of clauses 6.1, 6.2 or 6.4.

7. Data privacy and confidentiality

7.1 "Confidential Information" means, with respect to a Party (**"Disclosing Party"**), all non-public confidential information relating to the Disclosing Party's business. SoSafe and the customer shall comply with clauses 7.1., 7.2., 7.3. and 7.4. when exchanging Confidential Information. Confidential Information shall be designated and/or marked as Confidential upon disclosure, with the proviso that information of which the receiving Party (**"Receiving Party"**) was aware or under the circumstances should have been aware that it is considered confidential or proprietary by the Disclosing Party shall be considered Confidential Information even if it has not been designated or marked as such. The Receiving Party shall keep the Confidential Information secret and treat it with at least the same degree of care as the Receiving Party uses to protect its own Confidential Information, but at least with reasonable care. The Receiving Party shall use the Confidential Information only for the exercise of rights and performance of obligations under the respective Awareness Building Agreement. Confidential Information shall only be disclosed to those employees and contractors of the Receiving Party who need to know such information. With regard to SoSafe, Confidential Information includes in particular evaluations of customer data, the exact procedures and configurations of the Awareness Training (if not publicly available), the agreed prices and discounts as well as the contents of the learning modules and pages

7.2Appropriate confidentiality measures shall be taken to protect the information concerned, required by the circumstances. At SoSafe these include in particular physical access restriction to the premises, including video surveillance, restriction of access rights to customer-specific notes, annotations etc. only for individual employees and only if they need to know about them in order to provide the service (need-to-know principle), and a comprehensive confidentiality agreement, which shall be signed by all employees of SoSafe.

7.3 Confidential information is not covered by point 7.1. if (i) it becomes generally accessible and this is not based on a breach of point 7.1. or 7.2. (ii) they were known to the Receiving Party prior to the time of receipt and the Receiving Party was allowed to use the Confidential Information freely and without any confidentiality obligation; (iii) the Receiving Party obtained the Confidential Information lawfully through a third party who is neither employed by the Disclosing Party nor otherwise associated with its company, and who has voluntarily and lawfully provided this information to the Receiving Party; (iv) the Receiving Party can prove that such information was independently developed by employees or personnel of the Receiving Party who did not have access to the relevant Confidential Information and that no Confidential Information was used to develop such information; and/or (v) it is required to be disclosed by law or court order or disclosure is ordered by an authority authorized to do so.

7.4 The obligations under clause 7.1. apply for five (5) years after the end of the respective Awareness Building Agreement.

7.5 The customer assures that he is entitled to collect, process and use the personal data of his employees within the scope of the use of the platform or other services provided by SoSafe on the basis of an agreement on awareness building. A breach of the obligations of the customer in this clause 7.5 shall also entitle SoSafe to terminate all contracts existing between the customer and SoSafe without notice.

7.6 The Parties will process personal data only in accordance with the applicable data protection regulations and the Data Processing Agreement attached as **Annex 2**. For detailed information on the data processed during the simulated phishing campaigns, e-learning, etc., please refer to the Data Processing Agreement. Details about the processing of personal data that SoSafe processes as a controller can be found in the Privacy Policy, which is non-contractual and may be modified from time to time, available at https://sosafe.de/datenschutz/.

7.7 Company related information of the Customer shall be stored anonymously to enable a comparison of the achieved results in case of a possible repetition of the awareness building or other solutions.

8. Cooperation obligations of the customer

8.1 The customer shall provide SoSafe with all necessary or requested documents and information for the smoothest possible implementation of the awareness building process immediately after conclusion of the contract. This includes in particular the transmission of the user list with the users (see definition part B section 1.2.), where phishing simulations shall be carried out and who shall have access to the e-learning.

8.2 The customer shall name a contact person responsible for the project implementation who can answer all queries and make all related decisions.

8.3 The customer shall ensure within the scope of his possibilities that e-mails from SoSafe are not prevented from being delivered; this includes in particular the so-called "white listing" of the domains and servers operated by SoSafe. SoSafe shall inform the customer about relevant information, which shall be observed if possible.

9. General clauses

9.1 The customer shall only be entitled to assign claims from or in connection with the business relationship with SoSafe with the prior written consent of SoSafe, § 354a HGB (German Commercial Code) shall remain unaffected.

9.2 The place of performance for all obligations resulting from the Awareness Building Agreement, including the payment obligations of the customer, shall be the place of business of SoSafe.

9.3 SoSafe has the right to name the customer as reference customer. The customer grants SoSafe the right to use the customer's logo and name in electronic, printed or other form for internal or external marketing activities, free of charge, unlimited in space and content and limited in time to the duration of the customer relationship. (E.g. on the Internet, in brochures, offers, presentations or press releases.)

9.4 Exclusive place of jurisdiction for all disputes arising from or in connection with the Awareness Building Agreement shall be the place of business of SoSafe. However, SoSafe shall also be entitled to sue the customer at his place of business.

9.5 The contractual relationship shall be governed solely by the laws of the Federal Republic of Germany with the exception of the United Nations Convention on Contracts for the International Sale of Goods (CISG). The law of the Federal Republic of Germany shall - as far as legally possible - remain applicable even if reference is made to the law of another state under German law (exclusion of the conflict of laws).

9.6. SoSafe reserves the right to modify the offered Awareness Building Services as well as these GTCs, as far as the respective modification is necessary to reflect changes that could not be foreseen at the time of conclusion of the respective Awareness Building agreement and the non-observance of which would affect the contractual balance between SoSafe and the client, in particular, if SoSafe (i) is obliged to ensure that the Awareness Building Services comply with the applicable law, in particular if the applicable law changes, (ii) in order to comply with a court decision or a decision of the authorities against SoSafe and/or (iii) has to adapt the Awareness

Building services due to mandatory safety-related aspects. At no time shall the change in services restrict SoSafe's performance of its main contractual obligations.

9.7. in cases other than clause 9.6. SoSafe shall notify the customer in advance of the changes to the GTC. As far as the customer does not object to their validity within four (4) weeks after notification, the amendments shall be considered as accepted with effect for the future. If the customer objects to the amendments, the contractual relationship shall be continued in its present form. SoSafe shall refer to the effect of silence in the notification.

9.8 Amendments and supplements to the Awareness Building Agreement, including these GTC, must be made in writing, subject to clauses 9.6. and 9.7.

9.9 If one of the clauses of these GTC is invalid, the validity of the remaining clauses shall remain unaffected.

Section B - Specific provisions for web-based services (platform and services provided through the platform)

1. Right of use and conditions of use

1.1 Unless the Awareness Building Agreement has been concluded via the SoSafe website and therefore an account has already been created, clients must create an account (hereinafter referred to as **"Account"**) at https://manager.sosafe.de in order to be able to access the Awareness Building services that are only made available online via the platform. When creating an account, the customer must first enter his professional e-mail address and his first and last name. The customer must also create a password. The registration information must be correct, up-to-date and complete. Alternatively, SoSafe may also create the account for the customer and send the password to the customer.

1.2 In addition to the customer, only users authorized by the customer (hereinafter referred to as **"Users"**) may use the awareness building services provided via the platform to the extent determined by Section A (2) and Section B (2). For this purpose, the Users must also create an account (hereinafter referred to as **"User Account"**), as described in Section 1.1. Each user may only register once and one (1) User Account must be created per user. The registration is free of charge. A User Account is to be created for a specific user and is not transferable to another person.

1.3 The registration as a User according to section 1.2 is only permitted to persons for whom the customer has been granted a license to use the Awareness Building Services. The simultaneous use of the same account via several end devices is not permitted. Unless expressively permitted by SoSafe, Users may not register themselves with private e-mail addresses, particularly free mail providers such as GMX, Web.de or Google Mail.

1.4 The customer is responsible for the compliance of all his users with the Awareness Building Agreement and these GTC, including how users use their user account. Any use of the

Awareness-Building Services must be exclusively for the customer's own operational purposes and within the scope of use.

1.5 The customer and his users are obliged to keep the login data, passwords, etc. of the accounts / User Accounts secret and not to pass on the access data to unauthorised third parties (or other users) and to log off after each registration. The same shall apply to the access data used for a registration via Single-Sign-On, with the exception that a manual logoff is not required after each access. Declarations and actions which are made or committed after a login via the Account / User Account with the password and the e-mail address of the customer or a user can be attributed to the customer even if he has no knowledge of them. An attribution is made in particular if the Customer or a User provides third parties (including family members) with access to the password or the Account / User Account intentionally or negligently. The Customer must inform the Provider immediately as soon as he/she becomes aware that unauthorized third parties have access to and are aware of access data.

1.6 In case of a justified suspicion that access data has become known to unauthorized third parties, SoSafe shall be entitled but not obligated for security reasons to independently change the access data of the customer or the user concerned at its own discretion without prior notice or to temporarily block the use of the account / user account. SoSafe shall immediately inform the customer or user about this and shall provide new access data within a reasonable period of time. The customer or user shall not be entitled to have the original access data restored. In case of a registration via Single-Sign-On only the access via this Single-Sign-On with the previous access data will be blocked and the customer or user can only log in via the new access data. These new access data can in turn be integrated into a Single-Sign-On.

1.7 The customer undertakes to ensure that the users refrain from the following:

- to publish or make available on the platform insulting, violence glorifying, discriminating, inhuman or defamatory contents;
- to publish or make available pornographic or racist content on the platform;
- to publish or make available content on the platform that violates youth protection laws or criminal laws;
- to perform actions that could block, overload or impair the proper functioning or appearance of the platform or the service modules (e.g. denial of service attacks);
- to publish or make available untrue or unsubstantiated content on the platform;
- to publish or make available on the platform commercial communication (e.g. spam) not approved by SoSafe in advance;
- to collect content or information from other users by means of automated mechanisms (such as bots, robots, spiders or scrapers) or to access the Platform or the service modules in any other way, unless the express prior authorization of SoSafe has been obtained;
- to operate illegal structured sales networks, such as snowball systems, on the platform or in the service modules;
- upload viruses or other malicious code;
- Obtain login information or access an account/user account that belongs to another user;
- to use legally protected content without being entitled to do so;
- to collect, use or process data of other users without being entitled to do so.

1.8 SoSafe is entitled to irretrievably delete contents which violate clause 1.7. In this respect the customer and user shall not be entitled to the reinstatement of already deleted contents.

1.9 If the customer or one of his users violates clause 1.7 or legal regulations, SoSafe may

- modify or delete contents;
- restrict the user account temporarily or block it permanently;
- prohibit the user from registering again under his or another name after the deletion of his user account.

These sanctions may be imposed by SoSafe without prior notice and without consulting the customer, even against the customer's express will or against the user's will. SoSafe shall inform the client and the user of the relevant sanctions by e-mail.

2. Rights of use and copyright

2.1 SoSafe grants the customer the locally unlimited, temporary, revocable, non-exclusive, non-sublicensable and non-transferable right to use the platform and the service modules and additional services made available on it for his own operational purposes for the number of users and the agreed scope of use as specified in the Awareness Building Agreement.

2.2. The Customer is not entitled (i) to rent, lease, lend, reproduce, resell or otherwise distribute or pass on the Platform or access to the Platform, including via the Internet or a downstream public or private data network; (ii) to use the Platform to develop other services; (iii) to activate or use components of the Platform for which the Customer has not been granted rights of use; (iv) to transfer the rights of use of the platform to third parties or to grant third parties access to the platform; (v) to change, translate, copy, decompile the program code of the platform, to examine its functions, except as far as legally imperatively permitted according to § 69d or § 69e UrhG (German Copyright Act); as well as (vi) to remove, conceal or change legal notices, in particular regarding industrial property rights of SoSafe.

2.3 Provided that SoSafe enables the customer to use the platform for individual materials (evaluations of e-learning, evaluations of phishing simulations, etc.).) via the platform or to provide the customer with such materials individually created for him for downloading or printing, SoSafe shall grant the customer, upon full payment of the agreed remuneration, the unlimited, revocable, non-exclusive, non-sublicensable and non-transferable rights of use, unlimited in time and place, for all materials individually created by SoSafe for the customer within the scope of this agreement, as far as the transfer is possible according to German law or the actual circumstances.

2.4 SoSafe reserves the right to use the aforementioned individual materials (with the exception of all third-party protected trademarks or signs) and in particular the knowledge gained therefrom for its own purposes.

3. Warranty

3.1 With regard to the use of the platform and the service modules and additional services provided via the platform, §§ 536 ff. BGB (German Civil Code) and the following clauses 3.2. to 3.5 apply:

3.2 Strict liability for initial defects pursuant to § 536a para. 1, 1st var. BGB (German Civil Code) is excluded. The fault-based liability of SoSafe shall remain unaffected.

3.3 The rectification of defects shall be carried out at SoSafe's discretion either by free rectification or by replacement delivery.

3.4 A termination of the customer according to § 543 Abs. 2 S. 1 No. 1 BGB (German Civil Code) due to failure to grant the contractual use shall only be permissible, if SoSafe has been given sufficient opportunity to remedy the defects and this has failed.

3.5 SoSafe shall not assume any warranty for the Internet access of the customer, especially for the availability and dimensioning of the Internet access. The customer shall be responsible for his Internet access to the transfer point of the service.

Annex 1: Service Level Agreement (SLA) of SoSafe GmbH

Version 18.08.2021

Introduction

Scope

The Service Level Agreement concretizes and specifies the quality as well as the scope of the services offered by SoSafe GmbH (hereinafter referred to as **"SoSafe"**). An agreement is concluded between SoSafe and the client for the provision of services in the field of employee training/awareness-building (hereinafter referred to as the **"main agreement"**). The service provider SoSafe and the service recipient (hereinafter referred to as **"client"**) are hereinafter jointly referred to as **"parties"**.

This document contains all relevant provisions and regulations by which the service description of the Awareness Building Services and the obligations to cooperate in the main contract between the parties are specified.

Validity for different awareness service packages

SoSafe principally offers four different awareness packages: Starter, Essential, Professional and Premium. Individual sections of this Service Level Agreement may only refer to individual packages. This is indicated by headings of the respective sections. A more concrete definition of the scope of services of the individual Packages follows hereafter. In addition, in some Packages it is possible to use only individual modules from these (e.g. only the e-learning from the Business Essential) - in this case the corresponding provisions of the respective Package apply analogously for the individual module.

Furthermore, SoSafe offers individual, additional services/features as an option. These are listed separately in the following.

The customer is only entitled to the Awareness Building services described in sections 3 and 5 of this SLA to the extent purchased.

Conditions and obligations to cooperate for the use of the services

General conditions and obligations to cooperate

Various components of the following service modules (clause 3) require access to SoSafe web pages with a web browser. In this respect only the following browsers are supported and their use is therefore a prerequisite for the provision of services: Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge and Microsoft Internet Explorer 11 in their respective current versions.

Specific requirements and obligations to cooperate

The specific prerequisites or cooperation obligations for the use of the Awareness Building Services are described in Section 3 for the respective service modules.

Service modules

The following sections describe the services offered by SoSafe and define the processes and organizational interfaces required for service provision.

Phishing simulation

The phishing simulation service module comprises the sending of a defined number of (pre-arranged) e-mails to users over the service period. These e-mails simulate real phishing e-mails to increase the users' awareness of IT security risks caused by phishing attacks. When a user clicks on a phishing element (e.g. image, link) in one of the simulated phishing e-mails, a web page is called up (hereinafter referred to as the "learning page"), which informs the user about the simulation and provides concrete information on how the respective e-mail could have been identified as a phishing attempt.

To ensure that all simulated phishing mails are delivered to all users to be trained in the training, the customer is required to set up a whitelisting. This is a duty of cooperation on the part of the customer, without which SoSafe cannot guarantee the provision of services. At this point, the customer shall therefore be responsible for ensuring that the simulated phishing mails actually arrive in their complete form in the users' mailboxes and can be used within the scope of the training measure. If the customer cannot influence the whitelisting itself (e.g. because the customer has commissioned an IT service provider to manage its IT systems), the customer must ensure that the whitelisting is nevertheless carried out.

The following steps must be taken for whitelisting:

- SoSafe's dedicated mail servers must be whitelisted in the receiving mail system to prevent the rejection of incoming e-mails.
- Any existing filter systems (e.g. secure mail gateway) must be configured in such a way that the simulated phishing mails are not marked as "junk" or "spam" and delivery to the users can be guaranteed.
- Any existing systems provided by the customer to protect access to the Internet from the user's end devices (e.g. web gateways, proxies, security settings of the operating system) must be configured in such a way that the undistorted display of the simulated phishing e-mails in the user's e-mail programs is guaranteed. Furthermore, these systems are to be configured so that the learning pages can be displayed via a web browser.

SoSafe provides instructions for the implementation of these steps. The instructions also contain all necessary technical information such as IP addresses and server names of the mail servers, URLs to be released for filter systems and systems for access protection.

Phishing Report Button

The Phishing Report Button service module is a functionality that allows users to report e-mails that are considered to be a potential phishing attack. The report is sent to an e-mail address defined by the customer in the form of a forwarding of the suspicious e-mail. Simulated phishing emails from SoSafe are not forwarded, but reported to SoSafe. The customer must specify an e-mail address where the forwarding is to take place.

The functionality is provided in the form of a Microsoft Office Add-In. In order for the Outlook add-in to load and function properly, different requirements must be met on the server and client side.

Client requirements

- The client must be one of the supported applications for Outlook add-ins. The following clients support add-ins:
    - Outlook 2013 or higher on Windows
    - Outlook 2016 or higher on Mac
    - Outlook under iOS
    - Outlook under Android
    - Outlook on the Web for Exchange 2016 or higher and Office 365
    - Outlook.com

- Alternatively Google Workspace
- The client must be connected directly to an Exchange server or to Office 365. When configuring the client, the user must select Exchange, Office 365 or Outlook.com as the account type. If a POP3 or IMAP connection is configured for the client, add-ins are not loaded.

E-mail server requirements

If the user is connected to Google Workspace, Office 365 or Outlook.com, this already meets all the requirements for the e-mail server. However, for users connected to an on-premises Exchange Server installation, the following requirements apply:

- The server must be Exchange 2016 or later.
- Exchange Web Services (EWS) must be enabled and accessible over the Internet. Many add-ins require EWS to function properly.
- The server must have a valid authentication certificate to issue valid identity tokens. New Exchange Server installations include a default authentication certificate.
- The client access servers must be able to communicate with AppSource to access add-ins from Microsoft AppSource.

A successful installation as well as a smooth roll-out of the Add-In can only be guaranteed if the customer uses the standard settings of the respective program and has no third-party application in operation that affects the functionality of the Add-In. Individual support by SoSafe during the setup of the add-in in a non-standard infrastructure is explicitly excluded. As an optional service, resources with appropriate expertise can be arranged. This requires a separate and explicit agreement between the parties involved.

Client / Server API Compatibility

The Outlook Add-in makes use of Exchange Web Services (EWS) or the Outlook REST API, in order to retrieve data from the user’s Outlook mailbox. The following sections state the availability of EWS and REST API for all supported Exchange Server/Outlook Client combinations and their effect on forwarding.

Exchange On-Premise

For all Exchange On-Premise servers (no hybrid deployment) we can only support EWS.

Exchange Online / Hybrid server deployments

For Exchange Online and hybrid deployments of Exchange servers we support the following EWS and REST API availability for the respective client/server combinations:

REST: REST API only
EWS: EWS only
Both: EWS and REST API

Windows

Windows		**Windows Outlook clients**			
		MS 365[1]	**Outlook 2019**	**Outlook 2016**	**Outlook 2013**
Server	Exchange Online	Both	Both	EWS	EWS
	Exchange 2019[2]	Both	Both	EWS	EWS
	Exchange 2016[2]	Both	Both	EWS	EWS

macOS

macOS		**macOS Outlook clients**		
		MS 365[1]	**Outlook 2019**	**Outlook 2016**
Server	Exchange Online	Both	Both	Both
	Exchange 2019[2]	Both	Both	Both
	Exchange 2016[2]	Both	Both	Both

Other

		Outlook clients			
		Android App	**iOS App**	**Desktop Browser**	**Mobile Browser**
Server	Exchange Online	REST	REST	Both	not supported
	Exchange 2019[2]	REST	REST	Both	not supported
	Exchange 2016[2]	REST	REST	Both	not supported

[1] Microsoft Office 365 subscription
[2] connected to Exchange Online (hybrid deployment)

Differences in forwarding via EWS and REST

Forwarding can be done in ".eml" or "split" mode, each of which brings the following differences. Depending on the available API and the configured forwarding mode, the following files are forwarded to the customer's email addresses:

	via REST	via EWS
.eml mode	• mail.eml	• mail.eml ○ for emails greater than 500 kB the add-in automatically switches to split mode
Split mode	• body.html • headers.txt • All attachments as the original files [3]	• body.html • headers.txt • attachments.txt [3] ○ contains information about the attachment's name, size, type, isInline

[3] If the email contains attachments

E-Learning

The e-learning service module comprises the possibility for all authorized users of a customer to access the agreed number of learning modules within the scope of service provision. The learning modules impart knowledge in the field of IT security and cover a wide range of sub-topics. The booked learning modules can be accessed via SoSafe's own learning platform or integrated into a customer's existing Learning Management System (LMS) via SCORM streaming. The learning modules are divided into learning videos and interactive learning modules.

The learning videos can be used with or without acoustic output (this can be controlled locally via the user's operating system or browser). All language versions (see section "Multilingual Package") of the learning videos have an audio track and subtitles. The interactive learning modules are without sound track.

Access via learning platform

The proprietary learning platform of SoSafe is available at https://elearning.sosafe.de. Here users can register with their professional e-mail addresses. Alternatively, an anonymous access code can be used.

Access via customer-side LMS

The learning modules are provided in the standard SCORM 1.2 (compatible with common LMS such as: SAP SuccessFactors Learning, Adobe Captive Prime LMS, ILIAS, Moodle, Totara Learning) as container files. These container files can be integrated into the LMS. The content of the learning modules is then provided by a streaming server of SoSafe at the time of access. For this purpose, access to the streaming server at lms0.sosafe.de must be guaranteed. The content of the learning modules is always kept up-to-date by SoSafe, which means that both error corrections and updates to the latest state of knowledge ("state-of-the-art") in the field of IT security are carried out.

SoSafe Manager

The SoSafe Manager can be accessed by the customer at https://manager.sosafe.de. SoSafe Manager is the portal for the administration of awareness measures. Within the reporting dashboard on the portal, the customer can view various key figures about the commissioned service components, such as general click rates of the simulated phishing mails, the overall progress in e-learning or - depending on the service agreement - also individual e-learning results of individual employees. Exactly which data can be viewed and processed is regulated in a separate Data Processing Agreement.

Customer support

Communication channels

The general contact person for all SoSafe customers is the customer support. Customer users have the following options for submitting support requests:

- Support form incl. FAQ: https://support.sosafe.de
- E-Mail: support@sosafe.de
- Mail: SoSafe GmbH, Ehrenfeldgürtel 76, 50823 Köln, Deutschland

The administrators of the customers (section 8.2 of the GTC) also have the option to make support requests to the hotline (phone: +49 221 65083800).

All communication can take place in German or English - depending on the customer's requirements. Other languages are currently not offered on the support side.

Availability

Customer support is available Monday to Friday from 09:00 to 17:00, except on national holidays.

Response times

The response time principally begins with the receipt of a support request from a user or administrator by the customer support. The prerequisite for the start of the response time is a sufficiently specified description of the request or error in relation to the Awareness Building Services owed in each case..

The reaction times are subdivided according to benchmark values as follows:

- For general inquiries about the Awareness Building services owed: within two (2) business days
- In the event of disruptions to the Awareness Building services owed in each case (e.g. the service is only available to a limited extent): within one (1) working day

The classification of the support request according to the above mentioned subdivisions is done by the customer support, based on the error description of the customer.

Within the defined response time, the customer receives a qualified answer from the customer support. Ideally, this qualified answer already contains the solution or the completion of the process, but at least a first assessment of the support request and information about the further procedure.

In the event of a malfunction, the qualified response also contains information on the expected duration and extent of the reported malfunction as well as an initial approach to a solution.

Scope of services of individual awareness packages

The individual awareness packages of SoSafe contain different scopes of services and support levels. The special features of the individual packages are listed in the following sections. If services are not described in this SLA, the scope of services according to the feature overview on https://www.sosafe.de/produkt is of secondary importance

Package Starter

- The package Starter is only aivalable for customers with **5-250 users**.
- For package Starter, all users must be registered with the SAME mail domain name. (single domain only)
- The customer is provided with **instructions** (downloadable PDF) on the **self-service platform** https://app.sosafe.de, which explain all necessary steps, such as setting up whitelisting, in a way that is understandable for an average user.
- All relevant information (customer master data, billing data, etc.) must be entered by the customer via the platform.
- A template (Excel file) is provided for the transmission of the **user list**, the scheme of which must be adhered to to ensure a clean upload of the data to the self-service platform. This user list can be updated by the customer. The actual number of users in the system must not exceed the licensed number of users (contractually agreed upper limit).
- A sample of the Data Processing Agreement is provided, which must be signed and uploaded by the customer.
- **Interactive learning modules** and learning videos in e-learning are fixed and cannot be changed. A suitable industry package can be selected for the **phishing simulation.**.

Package Essential

- If required, a 30-minute **kick-off meeting** can be held by telephone or web conference in which a SoSafe awareness expert explains all necessary technical preparations to the customer and coordinates the next steps.
- Free choice of mail domain names for user registration.
- A template (Excel file) is provided for the transmission of the **user list** for the phishing simulation and/or e-learning, the scheme of which must be adhered to. The transmission of the user list to SoSafe is done via a secure data connection to the SoSafe Manager Portal. The customer will receive a user account for this purpose. The actual number of users available in the system shall not exceed the licensed number of users (contractually agreed upper limit). As a gesture of goodwill, a cost-neutral exceeding of the agreed upper limit by up to 7 % is granted.
- The customer can **update the user list** via the above-mentioned access to the SoSafe Manager Portal at any time on his own, should there be any changes due to fluctuation, etc.
- SoSafe provides instructions for setting up the **whitelisting**.
- For **e-learning**, the agreed upon number of learning modules and learning videos can be activated for all users of the customer from the available interactive learning modules on IT security (difficulty level: beginners). In consultation with the customer, SoSafe can be set up with a reminder function that, for example, reminds users who have not yet registered or have not yet completed individual modules by e-mail of a registration/finalization.
- For the **phishing simulation**, we randomly send out 12 simulated phishing emails throughout the year, based on attacks observed in your industry. This collection is updated continuously. Any customization of the e-mails' content is not included in this package; this is only possible in the Professional and Premium packages. Available languages are German and English.
- **Setup times**: The kick-off can be carried out within one calendar week from the date of order (written acceptance of the offer by SoSafe), or later if requested by the customer. As soon as the kick-off has been carried out, SoSafe assures a possible start of the awareness building within 10 working days, provided that all necessary data are provided by the customer without delay and that activities requiring cooperation are carried out.
- **User feedback**: You can view user feedback and export it as a CSV file.
- The evaluation contains **benchmarks** on all key figures compared to the customer average.
- When using the SoSafe learning platform, users receive a **certificate** for all learning modules passed.
- **Gamification**: On the SoSafe learning platform, users pass levels, collect badges and can view their progress in a personal success overview. (Can be switched on and off)

Package Professional

All components from Package Essential, but differently or additionally:

- **Spear phishing simulation**: All e-mails are individualized for the respective recipient using a placeholder system (e.g. "Dear Mr. Miller, ...") and in some cases also include details such as the name or location of the customer.

- **Branding**: The customer's logo is displayed at the top of the learning pages associated with the phishing simulation, as well as on the SoSafe learning platform. The buttons and colour design elements of the learning pages as well as the learning platform can be adapted in colour to the customer's corporate identity. In addition, the e-mail-unspecific information text on the learning pages can be created or adapted according to customer requirements. If logo and color scheme are freely available, the setup can be done by SoSafe. Otherwise, the corresponding data will be provided by the customer. The customer guarantees for the integration that he holds the rights of use of the logo and is liable for any violation of the rights of third parties.
- **Multilingual package**: Selected phishing emails, learning pages and learning content are available in additional languages. Currently 23 languages are available, an up-to-date list will be provided upon request.
- **Setup times**: The kick-off can be carried out within one calendar week from the date of order (written acceptance of the offer by SoSafe), or later if requested by the customer. As soon as the kick-off has been carried out, SoSafe assures a possible start of the awareness building within 20 working days, provided that all necessary data are provided by the customer without delay and that activities requiring cooperation are carried out.

Package Premium

All components from Package Professional, but differently or additionally:

- For the setup and configuration of the **Phishing notification button**, SoSafe will provide instructions for the technically supported infrastructure alternatives
- Selected **contents of the e-learning modules** can be customized. For this purpose, a questionnaire is provided, which allows the customer to define the individual features (e.g. password length, contact person for data protection) within a framework defined by SoSafe.
- **Customization Engine:** Selected contents of the e-learning modules can be customized. A questionnaire is provided for this purpose, which the customer can use to define the individual specifics (e.g. password length, contact person for data protection) within a framework defined by SoSafe.
- **Customized spear phishing simulation**: We additionally send 3 simulated phishing emails, which we create together with you individually for your organization (e.g. replication of a CEO fraud). The individually created phishing mails are provided in German and English.

Optional package Enterprise:

- **Targeted delivery**: We assign selected, simulated phishing emails to specific user groups for even more targeted training.
- **Full-service implementation**: Your personal implementation manager supports and advises you on the advanced configuration of your awareness platform: best-practice approaches, whitelisting, recommendations for communication incl. templates, user management with data quality assurance.

- **Business Review**: You will receive up to 4 Executive Business Reviews per year. This includes a 60 minute phone call with your personal manager at SoSafe. Furthermore, you will receive a report containing information on: 1) Target achievement (e.g. deep dive into relevant metrics and product usage data) 2) Benchmarking (e.g. against customer master data, industry of the customer, company size) 3) Advice on measures (e.g. providing communication documents to employees or for internal reporting, best practices of comparable companies) 4) Support and advice for the long-term cyber security awareness strategy of the customer.
- **Priority Support**: Your personal contact person treats all your support requests with priority and supports you by e-mail or telephone, subject to our support times.
- **ISO 27001 reporting**: The data is evaluated in a ISO 27001-audit compliant manner.
- **Expert evaluation**: In addition to the provisions regarding the **user list**, the list can be supplemented with additional classifications. These can be, for example, user groups based on the customer's organizational units or locations. The evaluations on the reporting dashboard are then differentiated according to this classification. When the customer defines the classification, the agreed provisions of the Data Processing Agreement must always be observed; for example, the minimum size of a user group must not be less than 5 persons for data protection reasons.
- **Expert benchmarking**: The evaluation contains additional benchmarks, e.g. on the customer's industry and company size.
- **Advanced scheduling**: We adapt the dispatch times individually to customer requirements, e.g. vacation periods and time zones.
- **SCORM streaming**: You get access to the learning modules as SCORM containers and can integrate them into your own learning management system.
- **Supporting awareness material**: You receive supporting digital material for your awareness campaign, e.g. posters, screensavers, flyers, communication templates.
- **Data export**: You can export evaluation data as Excel or CSV file.
- To register on the SoSafe learning platform, it is also possible to use a **Single Sign-On** via Azure Active Directory (AD) or Google. To enable the learning platform to authenticate itself against the AD, an Azure AD in the cloud is required (hybrid setup possible). The protocol used is OAuth 2.0 or SAML in version 2.0, which is ideally suited for use in web apps. Only a one-time authorisation of our web app by the customer's Azure AD administrator is required. The technical requirements for Single Sign-On can be viewed at support.sosafe.de. SCIM is supported within the following limits:
    - The SCIM connection to the SoSafe Manager only supports data transfers from the Microsoft Azure AD, no on-premise Active Directories are supported.
    - The SCIM connection only supports the connection of one Azure tenant. All user data to be transferred must be managed by the customer in one Azure tenant. The connection to multiple tenants is not supported.
    - If a SCIM connection to the SoSafe Manager is established, the user administration is carried out exclusively via the Azure AD on the customer side; it is not possible to additionally import users into the SoSafe database via Excel or CSV imports.

Package "Data Protection"

Can be booked in addition to or instead of the above packages.

Package "Data Protection Professional":

- For **e-learning**, the agreed upon number of learning modules and learning videos can be activated for all users of the customer from the available interactive learning modules . In consultation with the customer, SoSafe can be set up with a reminder function that, for example, reminds users who have not yet registered or have not yet completed individual modules by e-mail of a registration/finalization.
- If required, a 30-minute **kick-off meeting** can be held by telephone or web conference in which a SoSafe awareness expert explains all necessary technical preparations to the customer and coordinates the next steps.
- **User feedback**: You can view user feedback and export it as a CSV file.
- The evaluation contains **benchmarks** on all key figures compared to the customer average.
- When using the SoSafe learning platform, users receive a **certificate** for all learning modules passed.

Package "Data Protection Premium":

- **Customization Engine:** Selected contents of the e-learning modules can be customized. A questionnaire is provided for this purpose, which the customer can use to define the individual specifics (e.g. password length, contact person for data protection) within a framework defined by SoSafe.
- **Branding**: The customer's logo is displayed at the top of the learning pages associated with the phishing simulation, as well as on the SoSafe learning platform. The buttons and colour design elements of the learning pages as well as the learning platform can be adapted in colour to the customer's corporate identity. In addition, the e-mail-unspecific information text on the learning pages can be created or adapted according to customer requirements. If logo and color scheme are freely available, the setup can be done by SoSafe. Otherwise, the corresponding data will be provided by the customer. The customer guarantees for the integration that he holds the rights of use of the logo and is liable for any violation of the rights of third parties.

Optional Package "Data Protection Enterprise":

- **Full-service implementation**: Your personal implementation manager supports and advises you on the advanced configuration of your awareness platform: best-practice approaches, whitelisting, recommendations for communication incl. templates, user management with data quality assurance.
- **Business Review**: You will receive up to 4 Executive Business Reviews per year. This includes a 60 minute phone call with your personal manager at SoSafe. Furthermore, you will receive a report containing information on: 1) Target achievement (e.g. deep dive into relevant metrics and product usage data) 2) Benchmarking (e.g. against customer master data, industry of the customer, company size) 3) Advice on measures (e.g. providing communication documents to employees or for internal reporting, best

practices of comparable companies) 4) Support and advice for the long-term cyber security awareness strategy of the customer.

- **Priority Support**: Your personal contact person treats all your support requests with priority and supports you by e-mail or telephone, subject to our support times.
- **Expert evaluation**: In addition to the provisions regarding the **user list**, the list can be supplemented with additional classifications. These can be, for example, user groups based on the customer's organizational units or locations. The evaluations on the reporting dashboard are then differentiated according to this classification. When the customer defines the classification, the agreed provisions of the Data Processing Agreement must always be observed; for example, the minimum size of a user group must not be less than 5 persons for data protection reasons.
- **Expert benchmarking**: The evaluation contains additional benchmarks, e.g. on the customer's industry and company size.
- **Advanced scheduling**: We adapt the dispatch times individually to customer requirements, e.g. vacation periods and time zones.
- **SCORM streaming**: You get access to the learning modules as SCORM containers and can integrate them into your own learning management system.
- **Supporting awareness material**: You receive supporting digital material for your awareness campaign, e.g. posters, screensavers, flyers, communication templates.
- **Data export**: You can export evaluation data as Excel or CSV file.
- To register on the SoSafe learning platform, it is also possible to use a **Single Sign-On** via Azure Active Directory (AD) or Google. To enable the learning platform to authenticate itself against the AD, an Azure AD in the cloud is required (hybrid setup possible). The protocol used is OAuth 2.0, which is ideally suited for use in web apps. Only a one-time authorisation of our web app by the customer's Azure AD administrator is required. The technical requirements for Single Sign-On can be viewed at support.sosafe.de. SCIM is supported within the following limits:
  - The SCIM connection to the SoSafe Manager only supports data transfers from the Microsoft Azure AD, no on-premise Active Directories are supported.
  - The SCIM connection only supports the connection of one Azure tenant. All user data to be transferred must be managed by the customer in one Azure tenant. The connection to multiple tenants is not supported.
  - If a SCIM connection to the SoSafe Manager is established, the user administration is carried out exclusively via the Azure AD on the customer side; it is not possible to additionally import users into the SoSafe database via Excel or CSV imports.

Package „Work security"

- For **e-learning**, the agreed upon number of learning modules can be activated for all users of the customer from the available interactive learning modules on work security. In consultation with the customer, SoSafe can be set up with a reminder function that, for example, reminds users who have not yet registered or have not yet completed individual modules by e-mail of a registration/finalization. Available languages are German.

Package „General Act on Equal Treatment"

- For **e-learning**, the agreed upon number of learning modules can be activated for all users of the customer from the available interactive learning modules on the General Act on Equal Treatment. In consultation with the customer, SoSafe can be set up with a reminder function that, for example, reminds users who have not yet registered or have not yet completed individual modules by e-mail of a registration/finalization. Available languages are German.

Package „Compliance"

- For **e-learning**, the agreed upon number of learning modules can be activated for all users of the customer from the available interactive learning modules on compliance. In consultation with the customer, SoSafe can be set up with a reminder function that, for example, reminds users who have not yet registered or have not yet completed individual modules by e-mail of a registration/finalization. Available languages are German.

Service availability

General availability

For Awareness Building Services provided by SoSafe via https://elearning.sosafe.de, the learning pages or the streaming server as well as the phishing report button, the following average (based on the monthly average) availabilities must not be undercut. These are deemed to be fulfilled as long as the actual availability does not fall below this value on a monthly average.

Availability is measured as the ratio of uptime - the time the service is properly available - to total time, i.e. uptime plus downtime:

Availability = Uptime / (Uptime + Downtime)

Availability in percent - converted into minutes for a system that is available 24 hours a day, 365 days a year (24 × 365) (8760 hours).

- E-Learning-Plattform: 97 %
- SoSafe Streaming-Server (access via external LMS): 97 %
- Learning pages for simulation: 97 %
- Phishing report button/add-In: 97 %

Exceptions to availability

Maintenance work on the systems of SoSafe and its suppliers, which is necessary for the maintenance and security of the current operation or the implementation of updates or upgrades, shall not be considered as downtime in the sense of the aforementioned.

As a rule, maintenance is carried out on weekends between 09:00 on Saturday and 18:00 on Sunday or at night on every weekday between 23:00 and 07:00 the next morning. In exceptional cases, system maintenance can also be carried out at all other times, taking into account the least possible impairment of ongoing operations. In such cases SoSafe shall inform the customer about planned system maintenance as early as possible, but at the latest one calendar week before the system maintenance.

Failure to meet availability

For each shortfall of one full percentage point in the monthly General Availability, unless excluded under "Exceptions to availability", the customer shall receive one additional day of the agreed services at the end of the contract term.