1 General provisions

These "Offer Conditions for Security Options" apply to the Internet Security, Identity Security and Secure Internet Traffic services (hereinafter "Service" or "Services") of Swisscom (Switzerland) Ltd (hereinafter "Swisscom"). They apply in addition to the contractual provisions already existing between the customer and Swisscom, in particular the "General Terms and Conditions of Swisscom for Business Customers" ("GTC"), available at www.swisscom.ch/b2b-legal.

2 Swisscom services

2.1 General

The services can be individually subscribed to and combined as desired.

2.2 Scope of services Internet Security

The Internet Security service is offered in the form of a subscription, which can be used to protect up to ten devices (see https://www.swisscom.ch/sme-security).

The Internet or e-mail provider is responsible for network-side filters, e.g. spam and virus filters for e-mail.

Internet Security includes the following functions for Windows:

- Internet Security protects against attacks from the Internet in which unauthorised persons attempt to gain access to the customer's data and/or programs. It does this by using its own firewall or in conjunction with the firewall functions provided by the Windows operating system.
- Internet Security protects against malware such as viruses, spyware, worms, Trojans and rootkits, which unauthorised individuals use in an attempt to damage or misuse the customer's data and/or programs.
- Internet Security allows restrictions on the access of individual users to the Internet by means of password-protected or profile-based blocking of certain websites, maintenance of white and black lists to allow or block websites individually and entry of permitted surfing times.

Internet Security includes the following functions for Mac:

- Internet Security protects against viruses, worms and other malware.
- Internet Security removes secretly installed software from the customer's computer.
- Internet Security allows restrictions on the access of individual users to the Internet by means of password-protected or profile-based blocking of certain websites, maintenance of white and black lists to allow or block websites individually and entry of permitted surfing times.

Internet Security includes the following functions for Android (smartphone and tablet):

- Internet Security protects against viruses, worms and other malware.
- Internet Security identifies unsafe websites.
- Internet Security allows individual users' access to unwanted websites to be restricted using browser protection. In addition, programs (apps) can be blocked with the help of a programmable application control.
- Internet Security offers comprehensive anti-theft protection and allows the Android device to be blocked or reset via remote access and an audible alarm to be played on the stolen or lost device.

Internet Security includes the following functions for iOS (iPhone and iPad):

- Internet Security identifies unsafe websites and protects during online banking and shopping.
- Internet Security allows restrictions on the access of individual users to the Internet by means of password-protected or profile-based blocking of certain websites, maintenance of white and black lists to allow or block websites individually and entry of permitted surfing times.

An Internet Security licence can be used for another device at any time.

An up-to-date overview and details of the various functionalities can be found at https://www.swisscom.ch/sme-security .

2.3 Scope of services Identity Security

Cyber Identity Security provides protection against data theft and secures digital identities to protect them against cyber crime.

- A maximum of 10 mail addresses can be monitored for suspicious activity.
- The personal data linked to the e-mail addresses (e.g. e-mail address, user names, passwords, ID number, credit card numbers) is permanently monitored.
- In the event that the data linked to the e-mail address is stolen or misused, the customer is proactively alerted and receives immediate instructions to limit the damage.
- A password manager stores passwords securely in a vault, with synchronisation function for all devices
- The password manager also helps to create strong passwords. Only one master password is required.

An Identity Security licence can be used for a different e-mail address or credit card number at any time by deleting an existing e-mail address or credit card number in the app.

2.4 Scope of services Secure Internet Traffic

Secure Internet Traffic grants the Customer the use of a software-based security solution from the company Zscaler Inc. (based in California, USA; hereinafter referred to as "Zscaler"). The customer purchases a licence for each end device that they wish to protect and installs the associated device application. The service is provided in the form of a cloud solution in the standard Internet traffic route and analyses the user's incoming and outgoing web traffic (content) for different types of threats. The user's https-encrypted web traffic is also decrypted for this purpose in Zscaler's cloud solution and then re-encrypted after analysis. Several security techniques are applied to detect threats and defend against them.

A Secure Internet Traffic licence can be used for another device at any time. Customers can manage their own licences themselves via My Swisscom Business.

2.5 Scope of Services for Mail Security

Mail Security filters the customer's incoming and outgoing e-mails, providing protecting against a wide range of threats. In addition to detecting spam and viruses, Advanced Threat Protection (ATP) can provide protection against targeted and highly complex threats such as ransomware, blended and targeted attacks, and phishing attacks. ATP uses sandboxing, innovative forensic analysis engines, URL rewriting and URL scanning to detect dangerous e-mails. If attacks are detected, the user is notified in real time.

A combination of technical methods, signature-based scanning engines and heuristic methods are used to detect these threats.

With Mail Security, all e-mail addresses of a domain, which must be named when ordering the product, are automatically protected. It is not possible to protect individual e-mail addresses belonging to a domain. It is also not possible to exclude individual e-mail addresses from protection.

2.6 Updates

With Internet Security, the components of the services needed to detect viruses and other harmful programs are continuously and automatically updated. This is done to adjust the protection functions to known threats with the least amount of restrictions on the use of online services.

Identity Security requires updates to the application. These are performed independently of the detection and alerting of exposed or stolen private data.

Secure Internet Traffic also requires updates to the application. The application in the cloud, which carries out the data check, is continuously updated automatically and without limiting the functionality.

Mail Security does not require an application to be installed by the customer. The application in the cloud, which carries out the data check, is continuously updated automatically and is done so without limiting the functionality.

The customer is provided with new versions of the corresponding software free of charge.

2.7 Fault acceptance and support

If faults occur in the services' basic functionalities, the Swisscom Helpdesk is available to the customer free of charge for support.

Support units are available for problems with end devices and private infrastructure subject to a fee.

3 Performance and obligations of the customer

3.1 General conditions of use

Internet Security & Identity Security

Subscribing to the service(s) requires a fixed network or mobile subscription with Swisscom and activated access to My Swisscom Business.

Secure Internet Traffic & Mail Security

Subscribing to the service(s) requires an "inOne SME office" subscription with Swisscom and activated access to My Swisscom Business.

3.2 System requirements and updates

The end device in question must comply with the system requirements before the software can be used. A continuously updated overview of the system requirements can be obtained from the Swisscom portal (https://www.swisscom.ch/sme-security).

In order to use the full scope of each service, the customer must install all updates during the entire term of the subscription, use the current version of the software in each case, use an operating system that meets the current system requirements and keep it constantly up-to-date.

When installing a new version of the software, the customer may determine the time of installation themselves – with reservation to any effects on the scope of services. A new version of the software may include a change in system requirements. The customer undertakes to inform themselves periodically about the system requirements.

3.3 Downloading the software

In some cases it may be necessary to install software from the company F-Secure (Internet Security) or Zscaler (Secure Internet Traffic) in order to use the services.

When activating the software, the customer concludes a licence agreement with the respective software producer directly, which primarily regulates technical issues regarding use of the software and the processing of data by the software producer in question.

The customer is responsible for downloading the software where necessary, as well as for the necessary hardware and software components and computer configurations.

3.4 Impact on other services

The customer accepts that some online services may not be available or may be limited as a result of the use of the Services and their security settings.

4 Prices / billing

4.1 Prices

The current prices and charges published on https://www.swisscom.ch/sme-security or on the product page of the fixed network or mobile phone subscription of Swisscom.

The services listed here are invoiced pro-rata basis. One exception with Mail Security is, however, that the mail addresses that go beyond the basic package, as these are always invoiced for an entire month. The cut-off date is the 27th of the month. The highest number of e-mail addresses of a domain in the respective month will be invoiced on the due date.

4.2 Billing

All services described here are invoiced monthly on the customer's Swisscom bill.

Unless otherwise agreed, the payment obligation begins with the activation of the service in the My Swisscom Business or in other Swisscom ordering systems.

4.3 Payment default

If the customer does not pay the invoice by the due date or submit written, supported objections to it, they shall automatically be in default. In addition to other contractually and legally defined consequences of default, Swisscom may, to the extent permitted by law, interrupt the provision of all services, take further measures to prevent growing damage and/or terminate the contract without notice or compensation.

5 Intellectual property

The customer shall, for the duration of the contract, be granted a non-transferable, non-exclusive right to apply and use the subscribed service(s). All rights to existing intellectual property or intellectual property arising from performance of the contract by Swisscom or by authorised third parties shall remain with Swisscom or the authorised third parties. Should the customer violate third-party intellectual property rights and if claims are made against Swisscom in this respect, the customer shall hold Swisscom harmless.

6 Licence conditions of the software producer; Data collection, processing and storage

6.1 Licence conditions of the software producer

Within the scope of the services described, the activities performed by Swisscom relate primarily to the provision of rights to use the services of the respective software manufacturers in accordance with their terms and conditions. Swisscom warrants that it is entitled to grant the contractually agreed rights to the customer and that the performance of the respective software producer and the functions contained therein are available in accordance with the software producer’s specifications during the term of the contract. Swisscom shall have any defects reported by the customer immediately after discovery rectified by the software producer within a reasonable period of time. If this fails, the customer may, after the unsuccessful expiry of a further grace period, demand an appropriate price reduction from Swisscom in the case of insignificant defects or, in the case of significant defects, terminate the contract extraordinarily (ex nunc) and demand a pro rata refund in the case of prepaid services. The customer shall have no further claims.

Within the scope of the respective licence conditions of the software producer, other documents designated by the software manufacturer apply, which the customer accepts directly vis-à-vis the respective software manufacturer.

Any data transmissions between the customer and the respective software producer based on the usage of its software/services do not form part of this agreement and Swisscom assumes no responsibility for them. The respective software producer is not a subcontracted data processor or auxiliary partner of Swisscom regarding such data transmissions. The software producer's Privacy Policy shall apply in this respect; this is referred to in the EULA or other accompanying documents (listed below). It is the sole responsibility of the customer to assess the legality and suitability of such data transfers for their purposes and, if necessary, to restrict them via technical measures or settings in the product. This regulation also applies to any support cases handled with the assistance of Swisscom, in which Swisscom may make the customer's data accessible to the software producer on behalf of the customer.

6.2 Internet Security and Identity Security

The F-Secure EULA (https://www.f-secure.com/de/legal/terms), which the Customer accepts directly vis-à-vis F-Secure, shall also apply within the scope of the licensing.

You can see how F-Secure processes data in the "Privacy Policy for F-Secure Internet Security" (https://www.f-secure.com/de/legal/privacy/consumer/total) for Internet Security and in the "Privacy Policy for Identity Protection" (https://www.f-secure.com/de/legal/privacy/consumer/id-protection) for Identity Protection.

6.3 Secure Internet Traffic

The zScaler EULA (https://www.zscaler.com/legal/end-user-subscription-agreement), which the Customer accepts directly vis-à-vis F-Secure, shall also apply within the scope of the licensing

In the context of the present service, Swisscom's performance consists mainly of granting the right to use the services of Zscaler. Swisscom warrants that it is entitled to grant the contractually agreed rights to the customer and that the performance of Zscaler and the functions contained therein are available in accordance with Zscaler's specifications during the term of the contract. Swisscom shall have any defects reported by the customer immediately after discovery rectified by Zscaler within a reasonable period of time. If this fails, the customer may, after the unsuccessful expiry of a further grace period, demand an appropriate price reduction from Swisscom in the case of insignificant defects or, in the case of significant defects, terminate the contract extraordinarily (ex nunc) and demand a pro rata refund in the case of prepaid services. The customer shall have no further claims.

Any data transmissions between the Customer and Zscaler based on the use of Zscaler's services do not form part of this Agreement and Swisscom assumes no responsibility for them. The relevant data protection regulations of Zscaler apply. Reference is made to these in the EULA, other accompanying documents or on the Internet presence of Zscaler (https://www.zscaler.com/privacy/overview). It is the customer's responsibility to assess the legality and suitability of such data transfers for their purposes and, if necessary, to restrict them via technical measures or settings in the product.

Furthermore, the customer acknowledges and accepts that by using Secure Internet Traffic, ZScaler processes their Internet data traffic (in particular decryption, content analysis, re-encryption and retransmission or suppression of data traffic) abroad and the secrecy of telecommunications does not apply to this. The customer therefore consciously waives the secrecy of telecommunications to the extent of the use of Secure Internet Traffic and is responsible for informing all users to whom they make the service accessible of this circumstance in advance in an appropriate manner.

6.4 Mail Security

The Mail Security Service is provided in geo-redundant data centres in Switzerland in cooperation with a technology partner based in Germany (in the EU/EEA).

Physical data storage: The log data of the Mail Security Service is stored in data centres in Switzerland. Incoming and outgoing e-mails are only stored temporarily on the Mail Security Platform until they can be delivered to the corresponding mail server, following which they are deleted. Log data from e-mail filter activity is stored for 12 months and then deleted automatically.

Automatic data processing includes the metadata of message transmission (e-mail address of sender and recipient, e-mail subject, date/time of e-mail receipt and - delivery, IP addresses of the servers involved in the communication, SMTP error code and text), content of the e-mails and classification of the mail (clean, spam, virus, info mail). Data is processed on our own hardware, which is located in Swisscom data centres (colocation). No other data (mail header, sender, addressee, subject, date, text content) is passed on to third parties. Apart from the contractor and designated representatives of the customer, no third parties have access to the data. When using Advanced Threat Protection (sandbox), the customer consents to the transfer of data requiring analysis to the infrastructure of the application producer located in the EEA.

The 3rd level support of the application producer will have access to application data from abroad during support cases. Access will be provided by Swisscom selectively and only for the purpose in question (support and release cases). Access is only provided for the purpose of contract fulfilment. For spam and malware detection, the Mail Security Service exchanges metadata and content data of the e-mails with the central system of the application producer located abroad. By using the service, the customer agrees to such processing.

To analyse problems, it may be necessary for Swisscom to gain access to the customer's log files. If Swisscom is unable to rectify the problem itself, it is entitled to make the necessary customer service data available to the application producer located abroad (via an encrypted channel), so that the problem can be analysed.

7 Guarantees

With each service, Swisscom and the software producer shall ensure security in accordance with the current state of the art and within the scope of

the service (see Sections 2.2 to 2.5) depending on the service purchased or the operating system.

Swisscom endeavours to provide its services with high availability. However, in addition to the existing contractual provisions between Swisscom and the customer, **Swisscom does not offer any guarantee that the individual protection functions (see Sections 2.2 to 2.5) guarantee absolute protection. In particular, Swisscom offers no guarantee that the Services will detect or prevent every harmful event.**

In addition, Swisscom does not provide any guarantee

- of the uninterrupted and trouble-free functioning, quality and availability of the services and its individual functionalities at all times;
- perfect functioning of the services on all end devices and in combination with all hardware and software components and operating systems;
- that attacks, third party access or damaging programs do not impair the use of other services or otherwise harm the customer.
- the functionality of the services on devices that were not purchased from Swisscom or that are not on the list of supported devices.

8 Liability

Swisscom accepts no liability,

- if damage occurs or undesirable websites are accessible on the protected device despite the presence of installed and updated software;
- if Identity Security fails to detect a malware event and damage occurs as a result;
- if Mail Security fails to detect a malware event, and damage occurs as a result of this.

Swisscom excludes any liability - e.g. for damage in the form of loss of data, loss of passwords, loss of profit or consequential damage - to the extent permitted by law.

Nor shall it be liable for damage arising from the unlawful use of its services or any use that is in breach of contract.

Swisscom shall not be liable if service provision is disrupted, wholly or partially restricted or impossible due to force majeure. Force majeure particularly includes power outages and the occurrence of malware (e.g. virus attacks).

9 Duration and termination; promotions

9.1 Duration and termination

The services may be terminated by either party at any time. There is no minimum contract term for the security products described here.

If the fixed network or mobile subscription (3.1) existing at the time of the service's conclusion is terminated, services subscribed to in accordance with these offer conditions shall also be terminated explicitly in accordance with this section without further notice on the same date.

9.2 Promotions

The customer can only claim a promotion once for the service in question. The service automatically becomes subject to a fee after the promotion expires. Termination of the service at the end of the promotion does not entitle the customer to another free promotion. A further free promotion is also not applicable if the customer subscribes to the service again at a later date.

10 Changes

Swisscom reserves the right to amend the prices, services and offer conditions at any time. Swisscom shall notify the customer in an appropriate manner of any changes that are a disadvantage to the customer.

Should Swisscom increase its prices such that this leads to a higher overall cost for the customer or should Swisscom significantly change a service purchased by a customer or the offer condition to the disadvantage of the customer, the customer may cancel the affected service prematurely until the change enters into force without any financial consequences. If it fails to do so, it will be deemed to have accepted the changes. Price adjustments as a result of a change in the tax rates (e.g. if VAT is increased) as well as any price increases by third-party providers (especially in the case of value-added services) are not deemed to be price increases and do not constitute a right of cancellation. Should

Swisscom lower its prices, it may at the same time adjust any discounts granted before lowering its prices.