swisscom

**Offer conditions**
**Business Network Solutions**

## 1. Scope

These offer conditions are valid for Business Network Solutions from Swisscom (Switzerland) Ltd (hereinafter called "Swisscom“). The offer conditions for "Business Network Solutions“ apply in addition to the "General terms and conditions for service agreements, the "Special terms and conditions" for Internet and service and the offer conditions for "Smart Business Connect"; they have precedence over the latter in the case of contradictions.

## 2. General

### 2. 1 Requirements

The precondition in order for Business Network Solutions to function is an active connection of the service "Business Internet Services".
Business Network Solutions consists of a fixed component, "Managed Networks", as a basis that allows access to the Business Network Solutions dashboard where the options are independently configured and further options can be ordered.
Only the hardware stipulated by Swisscom may be used for Business Network Solutions.
A Business Network Solutions network may consist of several “Smart Business Connect” locations in Switzerland. The customer is the owner of the connection at the main site. This party is the contract holder for all locations. The first location for which Managed Networks are acquired will automatically be used as the main site. The main site may be altered later.

### 2. 2 Ordering, installation, configuration and support

Managed Networks must be acquired in the context the order for Business Internet Services. The remaining options must be independently acquired in the dashboard. By accepting the offer the customer agrees that the partner shall immediately be given the status of “technical admin” and can therefore order, cancel and configure options in the dashboard for all locations in the network.
The options will be installed on the customer's own responsibility or by a partner at a charge. Swisscom may arrange to find this partner for the customer. The installation of the options will lead to a marked interruption to the previous services. This interruption may last for quite some time. The customer shall not be entitled to any compensation or damage claims against Swisscom.
The proper configuration of Business Network Solutions is a matter for the customer and the partner. Technical conversions of the infrastructure necessitated by the change of solution are the customer's responsibility. It is the customer's responsibility to verify the extent to which this conversion will affect the services currently being supplied – also by third-party providers.
Services for configuration and integration on the basis of the customer's specific requirements shall be provided by Swisscom together with third parties (partners). The customer therefore agrees that Swisscom may provide the partner to be designated by the customer with the necessary data and system access. The partner shall initially be identified by the customer.
For a Business Network Solutions network the customer may only use one partner and will be given the status of “technical admin”. If the customer uses several partners, the customer shall be independently responsible for triaging and awarding the necessary access rights.
The 1st level support obligation shall be borne by the installing partner. The customer must contact the partner for support. If Swisscom is asked for support due to an interference caused by a faulty configuration of Business Network Solutions, the costs may be billed to the customer.

### 2. 3 Restrictions

Due to the activation of Managed Networks/Business Network Solutions, the data transmission speeds promised for Business Internet Services can no longer be guaranteed.
Existing fixed IP addresses for Business Internet Services must be re-ordered when ordering Business Network Solutions. The identical IP addresses can be ordered by the customer or the partner in the dashboard during a defined period. Entitlement to identical IP addresses lapses at the end of the period. The time limit will be displayed during the ordering process. In addition, the provisions of clause 3.1.4. also apply.
The activation of Managed Networks means that the configuration options on the Centro Business Router can no longer be used. Existing configurations will be lost. It is the customer's responsibility to save these configurations before activating the options and, if necessary, to re-configure them on the Business Network Solutions dashboard.
In order to guarantee that the Swisscom service are of the best possible quality, Swisscom will provide these

services with a static QoS configuration that cannot be altered.

## 3. Business Network Solutions options

The basic features of the options are described in the following. Detailed information and prices can be found in the service specifications and on the website. Unless otherwise described, the options will be charged to the location where the options are used.

### 3. 1 Managed Networks

Managed Networks makes it possible to network customer sites through access to the dashboard, to manage DHCP options and to operate a demilitarised zone (DMZ). In addition, "Network Address Translation“ rules (NAT) and "Port Access Translation“ rules (PAT) can be defined. The IP addresses required for this purpose have to be acquired separately.

### 3. 2 Managed Networks light

The Managed Networks light option contains the same functions as Managed Networks, but can only be used at a single company location, so networking with other locations is not included.
To use Managed Networks light at more than one location, the corresponding number of subscriptions is required. Here also, the service does not include networking between different locations. The Managed Networks option should therefore be chosen if you require VPN location networking.
Even so - especially with PWLAN, Blue TV Host and DCS Trunk (telephony) solutions - only isolated use is permissible, i.e. without networking with other company locations.

Accordingly, only the Managed Networks option may be used for VPN site networking, which must be observed in particular with Smart ICT, DCS and other data networking solutions such as RAS/S2S VPN etc.

Swisscom reserves the right to check that the Managed Networks light option is being used in compliance with the contract and, in cases of misuse, to charge difference in price between Managed Networks light and the Managed Networks option. The right is reserved to take other measures in accordance with the General Terms and Conditions.

### 3. 3 Managed Firewall Standard

The Managed Firewall Standard service makes it possible to define a set of rules for the outgoing data traffic from the LAN. It is possible to make a selection from various predefined security levels or to define a set of rules oneself. The independently defined set of rules will be lost as soon as the firewall is deactivated or another set of rules is selected.
In order to offer the greatest possible security, it is essential to order the option for all locations in the network. If locations are added to the network at a later date, the option will be automatically applied to these locations and billed additionally for these locations.

### 3. 4 Remote Access Services

With its Remote Access Services Swisscom offers a solution for accessing the company network independently of the location. Different two-factor authentication versions (SMS and mobile ID) are offered for this purpose. Details and terms of use for mobile ID can be found at http://documents.swisscom.com.
The configuration and the installation of the clients needed as well as the procurement of the terminals are entirely the responsibility of the partner and the customer. If the customer does not use the mobile ID devices provided by Swisscom it cannot be guaranteed that the services will function.
The use of the RAS client in public networks, in networks other than those of Swisscom or in networks abroad may involve risks such as eavesdropping by unauthorised third parties through network manipulation. The connection between the user and the Internet is not part of the RAS service. This has to be provided by the customers or users themselves through an Internet service provider (ISP). The quality of the service and the performance of the RAS depend on the quality of the connection provided by the ISP selected.
In order to maintain the security of Business Network Solutions, Swisscom helpdesks are not authorised to transmit any information concerning customer profiles, including users names, passwords etc. They cannot access this data, which is stored on secure servers. If a user requires such information, it must be retrieved by an authorised representative of the customer via the BNS dashboard.
For the Remote Access Service, including mobile ID, the terms and conditions of use for mobile ID apply in addition. These can be found on Swisscom's website.
The options will be charged to the main site.

3.5 Managed LAN
Managed LAN enables WLAN (Wireless Local Area Network) to be set up and administered within company networks with various user groups via the dashboard. The option must be ordered for each company location, if applicable, and will be billed per location. The hardware needed for this (access points, switches) must be obtained from Swisscom (service model with monthly charge). Swisscom ensures that the access points and switches represent the state of the art for the functions that are provided.
The aforementioned devices (access points, switches) remain the property of Swisscom. If the customer cancels a device provided as part of the service model or reports a defective device to Swisscom, Swisscom will inform the customer by when and to what address the device should be returned. If the customer fails to return the device to this address by the deadline indicated, Swisscom is entitled to charge the customer the time value of the device (standard current selling price subject to a five-year depreciation period).

3.6 Public WLAN (PWLAN)
3.5.1 General
PWLAN allows a customer to provide its guests with Internet access, combined with SMS user authentication. This chargeable option must be ordered for each company location at which the customer wants to use PWLAN. The customer is charged for each PWLAN access point license.

3.6.2 PWLAN basic
PWLAN basic enables you to login via SMS authentication and EAP SIM.

3.6.3 PWLAN advanced
PWLAN advanced allows you to personalise the PWLAN appearance.
With the options Voucher Login, Device Login and PMS Login, the legally required identification of the respective users is completed by the customer (essential contractual obligation of the customer). The customer guarantees the provision of the required personal identification information in a standard format determined by Swisscom, which is also suitable for automated further processing, for at least 6 months, calculated from the day on which the means of access was last used by the respective user. It also undertakes to transmit this information without delay in the event of a request (by Swisscom or the competent authority) for immediate or subsequent identification of users in surveillance procedures in accordance with the Federal Act on the Surveillance of Post and Telecommunications (SPTA, SR 780.1).

Voucher Login: With the Voucher Login, Swisscom has no information to identify the user. By providing a means of access, the customer is fully responsible for the correct and legally compliant identification of users, including the collection, storage, provision and transmission of personal data for the purpose of fulfilling or enabling fulfilment of legal obligations to provide information.

PMS Login The user credentials recorded by the customer are used for this login option, which is enabled by connecting the customer database via the SSH protocol to the PWLAN system of Swisscom. The customer is specifically responsible for:
•Procurement and implementation of all licenses for the required system(s) (SSH service, PMS, etc.)
•Provision, physical connection and the network connection, operation, maintenance of customer systems at the Swisscom “Peering Point”;
•Ensuring the functionality of the SSH service (including fault containment and restoration of proper operation);
•Identification of all users and collection of identification and personal data when providing the means of access (including the associated SSH or PMS login information)

Device Login: Registration of customer devices (MAC addresses) in the Business Center of Swisscom. In particular, the customer is obliged to maintain the MAC addresses (incl. updating these by adding or removing them) in the Swisscom Business Center without delay. The customer shall ensure that only devices used for the Device Login option are listed in the Swisscom Business Center, which are owned by the customer alone and predominantly used by the customer him/herself or on their behalf, and that they can identify such users at any time.

3.7 Managed Security
3.7.1 General information
Managed Security enables the setup and administration of firewalls and UTM (Unified Thread Management) services within company networks via the BNS dashboard.

If the customer orders the option, it is automatically activated by the partner at all locations of the customer and invoiced per location.

Responsibility for the security of the customer's systems lies with the customer/partner. Swisscom assumes no liability for the security settings configured by the partner/customer via the BNS dashboard.

3.7.2 Important option components
The most important components of the option are described below.

- Reporting
  Swisscom provides the customer/partner with a reporting module, which enables the customer/partner to access reports. Swisscom draws the customer's attention to the fact that it must inform its network users (such as employees or guests) in advance about the use of this reporting module, to ensure their personal rights are not violated. In this regard, it is advisable to issue monitoring regulations that provide information on the technical protective measures and protocols used, as well as on the usage and monitoring rules. Swisscom reserves the right to temporarily suspend or no longer offer the reporting module for technical or other reasons.
- Logging
  The log data recorded by the firewall is made available for download via the BNS dashboard. The customer itself is responsible for compliance with data protection legislation.
- Web filter
  The "web filter" is used to block access to certain websites with unwanted content. These filters are updated periodically. The customer has the possibility to block different categories of unwanted content. Swisscom excludes any liability and guarantee regarding the respective URLs and their categorisation as far as is legally permissible.
- External VPN connection point
  The External VPN connection point allows the customer to integrate a non-BNS location into the BNS company network. Responsibility for the locations, services and devices connected via the external VPN connection lies exclusively with the customer (or the partner commissioned by it). Swisscom assumes no responsibility for the security of sites connected via the external VPN connection or any malware entering the BNS network through these sites.

3.8 Special features in the case of fixed IP addresses within the framework of Business Network Solutions
In the case of Business Network Solutions fixed IP addresses must be acquired in the dashboard. There is no entitlement to certain IP addresses. IP addresses ordered in the dashboard cannot be adopted for Business Internet Services if the option or the underlying options, such as Managed Networks, are cancelled.
It should be noted that in the case of sub-networks of 4-64 fixed IP addresses 3 IP addresses are used for the technical provision of the service and can therefore no longer be used for customer-specific services. The options will be charged to the main site.

## 4. Prices, billing and discounts

The current prices, i.e. the one-off and recurring costs of the options, can be found on the Swisscom website. Existing discounts and promotions are not valid for Business Network Solutions. Traffic generated when using the Remote Access Service client will be charged for separately.

The obligation to pay for Managed Networks commences when the underlying Business Internet Service is activated. If the Business Internet Service is already active, the obligation to pay commences when an order is placed for Managed Networks. The obligation to pay for further options commences at the time when they are ordered.

## 5. Confidentiality and data protection

Swisscom reserves the right to access the dashboard in assurance cases or for purposes of maintenance and to store and evaluate all log data for the purpose of quality improvement.
On the activation of Business Network Solutions the customer hands over all network traffic to Swisscom (including traffic from the private network). Swisscom reserves the right to store and evaluate configuration data in order to improve the options.

In the event of support, Swisscom may grant foreign service providers temporary access to this service and the associated data such as WLAN credentials, configurations of the switches and access points of the customers (but not the respective identity of the customers). For service providers from a country with a lower level of protection (e.g. USA, India) than Switzerland, Swisscom ensures appropriate protection

with one or more measures pursuant to Art. 6 para. 2 DPA.

## 6. Guarantee

Swisscom will ensure that the components used are in line with the latest standards in order to support the functions that have been made available. In order to achieve the high security standards, Swisscom utilises appropriate security resources that are in line with the latest technology. The customer acknowledges the fact that, despite all efforts on the part of Swisscom and the use of modern technologies and observance of security standards, absolute security and fault-free service performance for the systems used cannot be guaranteed. Swisscom will also take measures to protect the infrastructure it uses against intrusion by third parties. However, 100% protection of the company network cannot be guaranteed.

## 7. Formation, duration and termination of the Agreement

### 7. 1 Formation of the contract, entry into force

When an option is ordered this will result in an addition to the existing contract. The customer is responsible towards Swisscom for the orders in the dashboard being executed by the customer or by a person authorised by the customer.

### 7. 2 Periods of notice and minimum subscription period

The Business Network Solutions options have no minimum subscription periods. Options ordered in the dashboard must be independently cancelled by the customer in the dashboard. Swisscom, for its part, may also use other channels for any cancellations.
The cancellation of the required Business Internet Service from Smart Business automatically cancels all connected options.
The cancellation of Managed Networks automatically cancels all options at the relevant location.
At the main site Managed Networks cannot be cancelled until all options have been cancelled at all other locations in the network.
The cancellation of an option automatically deletes all connected configurations. The configurations cannot be saved.

## 8. Changes and settings

The changes and the setting of Business Network Solutions and of individual options depends on the General Terms and Conditions and the Special Terms and Conditions.

February 2021