



### 1. Geltungsbereich

---

Diese Angebotsbedingungen finden auf Business Network Solutions von Swisscom (Schweiz) AG (nachstehend „Swisscom“) Anwendung. Die Angebotsbedingungen „Business Network Solutions“ gelten ergänzend zu den „Allgemeine Geschäftsbedingungen für Dienstleistungen („AGB“), zu den „Besonderen Bedingungen“ für Internet und Service und den Angebotsbedingungen „Smart Business Connect“ und gehen diesen im Falle von Widersprüchen vor.

### 2. Allgemein

---

#### 2.1 Voraussetzungen

Für die Funktionsfähigkeit von Business Network Solutions wird eine aktive Verbindung des Dienstes Business Internet Services vorausgesetzt.

Business Network Solutions besteht aus einem festen Bestandteil „Managed Networks“ als Grundlage, der den Zugriff zum Business Network Solutions Dashboard ermöglicht, in dem die Optionen selbständig konfiguriert und weitere Optionen bestellt werden können.

Für die Nutzung von Business Network Solutions ist ausschliesslich die von Swisscom vorgeschriebene Hardware zu nutzen.

Ein Business Network Solutions Verbund kann aus mehreren „Smart Business Connect“ Standorten in der Schweiz bestehen. Als Kunde gilt derjenige, der Inhaber des Anschlusses am Hauptstandort ist. Er ist Vertragsinhaber für sämtliche Standorte. Der erste Standort, für den Managed Networks erworben wird, wird automatisch als Hauptstandort verwendet. Der Hauptstandort kann nachträglich gewechselt werden.

#### 2.2 Bestellung, Installation, Konfiguration und Support

Managed Networks muss im Rahmen der Business Internet Services Bestellung erworben werden. Die restlichen Optionen müssen im Dashboard selbständig erworben werden. Durch das Akzeptieren der Offerte willigt der Kunde ein, dass der Partner umgehend den Status „Technical Admin“ erhält und der Partner damit für sämtliche Standorte des Verbunds Optionen im Dashboard bestellen und kündigen und konfigurieren kann.

Die Installation der Optionen erfolgt in eigener Verantwortung oder kostenpflichtig durch einen Partner. Dieser kann durch Swisscom vermittelt werden. Die Installation der Optionen führt zu einem merklichen

Unterbruch der bisherigen Services. Dieser Unterbruch kann eine längere Zeit beanspruchen. Es bestehen dabei keine Ersatz- oder Schadensersatzansprüche gegenüber Swisscom.

Die ordnungsgemässe Konfiguration von Business Network Solutions liegt in der Hand des Kunden und Partners. Technische Umstellungen der Infrastruktur, die durch den Wechsel der Lösung notwendig sind, liegen in der Verantwortung des Kunden. Die Prüfung, inwiefern diese Umstellung Auswirkung auf aktuell bezogene Dienstleistungen – auch von Drittanbietern – zur Folge hat, obliegt dem Kunden.

Dienstleistungen zur Konfiguration und Integration auf Basis von kundenindividuellen Anforderungen erbringt Swisscom gemeinsam mit Drittparteien (Partner), deshalb erklärt sich der Kunde bereit, dass Swisscom die notwendigen Daten und Systemzugriffe dem vom Kunden zu benennenden Partner zur Verfügung stellt. Der Partner wird initial vom Kunden identifiziert. Für einen Business Network Solutions Verbund darf der Kunde nur einen Partner einsetzen und erhält den Status „Technical Admin“. Falls der Kunde mehrere Partner einsetzt, ist er selbständig verantwortlich für die Triagierung und Vergabe der nötigen Zugriffrechte.

Die 1st Level Supportpflicht obliegt dem installierenden Partner. Für den Support hat sich der Kunde an den Partner zu wenden. Wird Swisscom wegen einer Störung in Anspruch genommen, deren Ursache in einer fehlerhaften Konfiguration von Business Network Solutions liegt, so können die Kosten dem Kunden in Rechnung gestellt werden.

#### 2.3 Einschränkungen

Durch die Aktivierung von Managed Networks/Business Network Solutions können die bei Business Internet Services versprochenen Datenübertragungsgeschwindigkeiten nicht mehr garantiert werden.

Bestehende fixe IP-Adressen bei Business Internet Services müssen bei Bestellung von Business Network Solutions neu bestellt werden. Die identischen IP Adressen können während einer definierten Frist im Dashboard durch den Kunden oder Partner bestellt werden. Nach der Ablauf der Frist erlischt der Anspruch auf identische IP Adressen. Die Frist wird im Rahmen des Bestellprozesses angezeigt. Im Übrigen gelten die Bestimmungen von Ziffer 3.1.4..

Durch die Aktivierung von Managed Networks können die Konfigurationsmöglichkeiten auf dem Centro Business Router nicht mehr genutzt werden. Bestehende



Konfigurationen gehen verloren. Es liegt in der Verantwortung des Kunden, diese vor Aktivierung der Optionen zu speichern und ggf. im Business Network Solutions Dashboard neu zu konfigurieren.

Um die bestmögliche Qualität der Swisscom Services zu gewährleisten, versieht Swisscom diese Services mit einer statischen QoS Konfiguration, die nicht geändert werden kann.

### 3. Business Network Solutions Optionen

Nachfolgend werden die Optionen in ihren Grundzügen beschrieben. Detailinformationen und Preise sind den Servicespezifikationen und der Website zu entnehmen. Falls nicht abweichend beschrieben, werden die Optionen auf den Standort verrechnet, an dem die Optionen verwendet werden.

#### 3.1 Managed Networks

Managed Networks ermöglicht durch den Zugriff auf das Dashboard Kundenstandorte zu vernetzen und DHCP Optionen zu verwalten und eine demilitarisierte Zone (DMZ) zu betreiben. Zudem können „Network Address Translation“ Regeln (NAT) und „Port Access Translation“ Regeln (PAT) definiert werden. Die dazu benötigten IP Adressen sind separat zu erwerben.

#### 3.2 Managed Networks light

Die Option Managed Networks light beinhaltet dieselben Funktionen wie Managed Networks, darf aber nur an einem einzigen Firmenstandort eingesetzt werden, ohne Vernetzung mit anderen Standorten.

Für den Einsatz an mehreren Firmenstandorten muss die entsprechende Anzahl Optionen Managed Networks light abonniert werden. Auch so ist - insbesondere bei PWLAN-, Blue TV Host- und DCS Trunk- (Telefonie) Lösungen - nur ein isolierter Einsatz, d.h. ohne Vernetzung mit anderen Firmenstandorten zulässig.

Für eine VPN-Standortvernetzung darf demnach nur die Option Managed Networks verwendet werden, was insbesondere bei Smart ICT-, DCS- und weiteren Datenvernetzungslösungen wie RAS/S2S VPN etc. zu beachten ist.

Swisscom behält sich vor, die vertragskonforme Nutzung der Option Managed Networks light zu überprüfen und im Missbrauchsfall insbesondere die Differenz zur Option Managed Networks nachzubelasten. Weitere Massnahmen gemäss AGB bleiben vorbehalten.

#### 3.3 Managed Firewall Standard

Der Managed Firewall Standard Service ermöglicht es, ein Regelset für den aus dem LAN ausgehenden Datenverkehr festzulegen. Es besteht die Möglichkeit, aus unterschiedlichen vordefinierten Sicherheitsstufen auszuwählen oder selbständig ein Regelset festzulegen. Das selbständig definierte Regelset geht verloren, sobald die Firewall deaktiviert wird, oder ein anderes Regelset ausgewählt wird.

Um die bestmögliche Sicherheit zu bieten, muss die Option bei Bestellung zwingend für alle Standorte im Verbund genommen werden. Werden zu einem späteren Zeitpunkt Standorte dem Verbund hinzugefügt, wird die Option automatisch auf diese angewendet und zusätzlich für diese in Rechnung gestellt.

#### 3.4 Remote Access Services

Die Swisscom bietet mit Remote Access Services eine Lösung, um unabhängig von Ort auf das Firmennetzwerk zuzugreifen. Es werden dazu unterschiedliche Zwei-Faktor-Authentisierung Varianten (SMS und Mobile ID) angeboten. Details und Nutzungsbestimmungen zu Mobile ID finden sich auf <http://documents.swisscom.com>.

Die Konfiguration und die Installation der benötigten Clients sowie die Beschaffung der Endgeräte sind vollumfänglich in der Verantwortung des Partners und Kunden. Verwendet der Kunde nicht die von Swisscom zur Verfügung gestellte Mobile ID, kann die Funktionsfähigkeit der Services nicht garantiert werden.

Die Nutzung des RAS Clients in öffentlichen Netzen, in anderen Netzen als Swisscom oder im Ausland kann Risiken bezüglich Abhörung mittels Netzmanipulation durch unbefugte Dritte mit sich bringen. Die Verbindung zwischen dem Benutzer und dem Internet ist nicht Teil des RAS-Service. Dieser ist über einen Internet Service Provider (ISP) vom Kunden oder Benutzer selbst zu beschaffen. Dabei sind die Qualität des Service und die Leistung des RAS von der Qualität der Verbindung abhängig, die von dem gewählten ISP zur Verfügung gestellt wird.

Um die Sicherheit von Business Network Solutions zu erhalten, sind die Swisscom Helpdesks nicht autorisiert, Informationen über Kundenprofile, einschliesslich Benutzernamen, Passwörter usw. zu übermitteln. Sie haben keinerlei Zugriff auf diese Daten, die auf sicheren Servern gespeichert sind. Benötigt ein Benutzer solche Informationen, müssen diese von einem autorisierten Vertreter des Kunden über das BNS Dashboard abgerufen werden.



Für den Remote Access Service inkl. Mobile ID gelten zusätzlich die Nutzungsbestimmungen Mobile ID, welche auf der Swisscom Website aufrufbar sind. Die Optionen werden auf den Hauptstandort verrechnet.

### 3.5 Managed LAN

Managed LAN ermöglicht das Aufsetzen und Administrieren von WLAN (Wireless Local Area Network) innerhalb Firmennetzwerken mit verschiedenen Nutzergruppen über das Dashboard. Die Option muss für jeden Firmenstandort, wo benötigt, bestellt werden und es wird pro Standort verrechnet.

Die dazu notwendige Hardware (Access Points, Switches) muss über Swisscom bezogen werden (Servicemodell mit Monatsgebühr). Swisscom stellt sicher, dass die eingesetzten Access Points und Switches für die bereitgestellten Funktionalitäten dem aktuellen Stand der Technik entsprechen.

Die erwähnten Geräte (Access Points, Switches) verbleiben im Eigentum von Swisscom. Kündigt der Kunde im Rahmen des Servicemodells ein Gerät oder meldet er Swisscom einen Geräte defekt, informiert Swisscom den Kunden, bis wann und an welche Adresse er das Gerät retournieren muss. Schickt der Kunde das Gerät nicht fristgerecht an diese Adresse, ist Swisscom berechtigt, dem Kunden den Zeitwert des Gerätes (aktueller marktüblicher Verkaufspreis, unter Anwendung einer fünfjährigen Abschreibungsdauer) in Rechnung zu stellen. Bei Beendigung des Vertragsverhältnisses verpflichtet sich der Kunde, die Infrastruktur in dem Zustand an Swisscom zurückzugeben, der sich aus dem vertragsgemässen Gebrauch ergibt.

### 3.6 Public WLAN (PWLAN)

#### 3.6.1 Allgemein

PWLAN ermöglicht es dem Kunden, seinen Gästen einen Internetzugang mit SMS Benutzerauthentifizierung zur Verfügung zu stellen. Die kostenpflichtige Option muss für jeden Firmenstandort, an welchem der Kunde PWLAN wünscht, bestellt werden. In Rechnung gestellt wird jede PWLAN Accesspoint-Lizenz.

#### 3.6.2 PWLAN basic

PWLAN basic ermöglicht das Login per SMS Authentifizierung und EAP SIM.

#### 3.6.3 PWLAN advanced

PWLAN advanced ermöglicht die Personalisierung des PWLAN-Auftritts.

Bei den Optionen Voucher-Login, Device-Login und

PMS-Login erfolgt die gesetzlich vorgeschriebene Identifikation der jeweiligen Benutzer durch den Kunden (wesentliche Vertragspflicht des Kunden). Der Kunde gewährleistet die Bereitstellung erforderlicher Personen-Identifikationsinformationen in einem von Swisscom bestimmten üblichen und zur automatisierten Weiterverarbeitung geeigneten Format während mindestens 6 Monaten, gerechnet ab dem Tag der letzten Nutzung des Zugangsmittels durch den jeweiligen Benutzer. Zudem verpflichtet er sich zur unverzüglichen Übermittlung dieser Informationen im Falle der Anforderung (durch Swisscom oder die zuständige Behörde) zwecks sofortiger oder nachträglicher Identifizierung von Benutzern in Überwachungsverfahren gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1).

Voucher-Login: Beim Voucher-Login liegen Swisscom keine Angaben zur Identifizierung der Benutzer vor. Der Kunde ist mit der Abgabe eines Zugangsmittels vollumfänglich verantwortlich für die korrekte und gesetzeskonforme Identifizierung von Benutzern, inklusive die Erfassung, Aufbewahrung, Bereitstellung sowie Übermittlung von Personendaten zwecks Erfüllung resp. Ermöglichung gesetzlicher Auskunftspflichten.

PMS-Login: Login mittels der kundenseitig erfassten Benutzer-Credentials durch Anbindung der Kundendatenbank via SSH-Protokoll an das PWLAN-System von Swisscom. Der Kunde ist namentlich verantwortlich für:

- Beschaffung und Implementierung aller Lizenzen für das(die) benötigte(n) System(e) (SSH-Service, PMS, usw.);
- Bereitstellung, physische Anbindung und Verbindung, Betrieb, Wartung kundenseitiger Systeme an den Swisscom "Peering Point";
- Sicherstellung der Funktionstüchtigkeit des SSH Services (inkl. Störungseingrenzung und Wiederherstellen des ordnungsgemässen Betriebs);
- Identifizierung aller Benutzer und Erfassung der Identifizierungs- und Personendaten im Zuge der Abgabe von Zugangsmitteln (inkl. zugehöriger SSH- resp. PMS-Login-Informationen).

Device-Login: Registrierung von kundenseitigen Geräten (MAC-Adressen) im Business Center von Swisscom. Der Kunde ist insbesondere verpflichtet zu unverzüglicher Pflege (inkl. Aktualisierung durch Hinzufügen resp. Entfernen) von MAC Adressen im Swisscom Busi-



ness Center. Der Kunde stellt sicher, dass ausschliesslich Geräte für Device-Login im Swisscom Business Center aufgeführt sind, welche in seinem alleinigen Eigentum stehen und überwiegend durch ihn selbst oder in seinem Namen genutzt werden und deren Benutzer er jederzeit identifizieren kann.

### 3.7 Managed Security

#### 3.7.1 Allgemein

Managed Security ermöglicht das Aufsetzen und Administrieren von Firewall und UTM (Unified Threat Management) Services innerhalb Firmennetzwerken über das BNS Dashboard.

Bestellt der Kunde die Option, wird sie durch den Partner automatisch an allen Standorten des Kunden aktiviert und pro Standort in Rechnung gestellt.

Die Verantwortung für die Sicherheit der kundenseitigen Systeme liegt beim Kunden/Partner. Swisscom übernimmt keine Haftung für die vom Partner/Kunden konfigurierten Security Einstellungen über das BNS Dashboard.

#### 3.7.2 Wichtige Optionsbestandteile

Nachstehend werden die wichtigsten Bestandteile der Option beschrieben.

- **Reporting**  
Swisscom stellt dem Kunden/Partner ein Reporting-Modul zur Verfügung, welches dem Kunden/Partner ermöglicht, auf Reports zuzugreifen. Swisscom macht den Kunden darauf aufmerksam, dass er seine Netzwerkbenutzer (wie z.B. Mitarbeiter oder Gäste) vorgängig über den Einsatz dieses Reporting-Moduls zu informieren hat, um deren Persönlichkeitsrechte nicht zu verletzen. In diesem Zusammenhang empfiehlt sich der Erlass eines Überwachungsreglements, worin über die eingesetzten technischen Schutzmassnahmen und Protokollierung sowie über die Nutzungs- und Überwachungsregelung informiert wird. Swisscom behält sich dabei das Recht vor, das Reporting-Modul aus technischen oder anderen Gründen vorübergehend einzustellen oder nicht mehr anzubieten.
- **Logging**  
Die von der Firewall registrierten Logdaten werden auf dem BNS Dashboard für den Download zur Verfügung gestellt. Der Kunde ist selbst für die Einhaltung der Datenschutzgesetzgebung verantwortlich.

- **Webfilter**  
Der "Webfilter" wird benutzt, um den Zugriff auf bestimmte Webseiten mit unerwünschtem Inhalt zu sperren. Diese Filter werden periodisch aktualisiert. Der Kunde hat die Möglichkeit, verschiedene Kategorien unerwünschten Inhaltes zu blockieren. Swisscom schliesst jegliche Haftung und Gewährleistung betreffend den enthaltenen URL's und deren Kategorisierung soweit gesetzlich zulässig aus.
- **External VPN Connection Point**  
Der External VPN Connection Point erlaubt es dem Kunden, ein nicht BNS Standort ins BNS Firmennetzwerk einzubinden. Die Verantwortung über die durch die External VPN Connection verbundenen Standorte, Services und Devices liegt ausschliesslich beim Kunden (bzw. bei dem von ihm beauftragten Partner). Swisscom übernimmt keine Verantwortung für die Sicherheit der über die External VPN Connection verbundenen Standorte oder Malware, die durch diese Standorte ins BNS Netzwerk gelangt.

### 3.8 Besonderheiten bei fixen IP Adressen im Rahmen von Business Network Solutions

Bei Business Network Solutions müssen fixe IP Adressen im Dashboard erworben werden. Es besteht kein Anspruch auf bestimmte IP-Adressen. Im Dashboard bestellte IP Adressen können im Falle einer Kündigung der Option oder der zu Grunde liegenden Optionen wie Managed Networks nicht für Business Internet Services übernommen werden.

Es gilt zu beachten, dass bei den Subnetzen von 4-64 fixen IP Adressen jeweils 3 IP Adressen für die technische Bereitstellung des Services benutzt werden und somit nicht mehr für kundenspezifische Services verwendet werden können. Die Optionen werden auf den Hauptstandort verrechnet.

## 4. Preise, Verrechnung und Rabatte

---

Die aktuellen Preise, d.h. einmalige und wiederkehrende Kosten der Optionen sind auf der Swisscom Website zu entnehmen. Bestehende Rabatte und Promotionen sind nicht auf Business Network Solutions anwendbar. Bei der Benutzung des Remote Access Service Client anfallender Traffic wird separat verrechnet.

Die Pflicht zur Bezahlung von Managed Networks beginnt zum Zeitpunkt der Aktivierung des zugrunde



liegenden Business Internet Services. Ist Business Internet Services bereits aktiv, so beginnt die Pflicht zur Bezahlung zum Zeitpunkt der Bestellung von Managed Networks. Die Pflicht zur Bezahlung der weiteren Optionen beginnt zum Zeitpunkt ihrer Bestellung.

### 5. Vertraulichkeit und Datenschutz

Swisscom behält sich vor, in Assurancefällen oder auf Grund von Wartungszwecken auf das Dashboard zuzugreifen und sämtliche Log-Daten zwecks Qualitätsverbesserungen zu speichern und auszuwerten. Durch die Aktivierung von Business Network Solutions übergibt der Kunde sämtlichen Netzwerkverkehr (auch aus dem privaten Netz) an Swisscom. Swisscom behält sich vor, Konfigurationsdaten zu speichern und auszuwerten, um die Optionen zu verbessern.

Im Supportfall kann Swisscom ausländischen Dienstleistern einen vorübergehenden Zugriff auf den vorliegenden Service und den damit zusammenhängenden Daten wie WLAN Credentials, Konfigurationen der Switches und Access Points der Kunden (jedoch nicht die jeweilige Identität der Kunden) einräumen. Bei Dienstleistern aus einem Land mit einem tieferen Schutzniveau (z.B. USA, Indien) als in der Schweiz stellt Swisscom mit einer oder mehreren Massnahmen gemäss Art. 6 Abs. 2 DSGVO einen angemessenen Schutz sicher.

### 6. Gewährleistung

Swisscom stellt sicher, dass die eingesetzten Bestandteile für die bereitgestellten Funktionalitäten dem aktuellen Stand der Technik entsprechen. Zur Erreichung eines hohen Sicherheitsstandards setzt Swisscom angemessene und dem aktuellen Stand der Technik entsprechende Sicherheitsmittel ein. Der Kunde nimmt zur Kenntnis, dass trotz aller Anstrengungen von Swisscom und des Einsatzes moderner Techniken und Sicherheitsstandards eine absolute Sicherheit und Fehlerlosigkeit der benutzten Systeme und Verfahren nicht gewährleistet werden kann. Swisscom trifft im Weiteren Vorkehrungen, um die von ihr eingesetzte Infrastruktur vor Eingriffen Dritter zu schützen. Ein absoluter Schutz des Firmennetzwerkes kann jedoch nicht gewährt werden.

### 7. Zustandekommen, Mindestbezugsdauer und Kündigung

#### 7.1 Zustandekommen, Inkrafttreten

Die Bestellung einer Option führt zu einer entsprechenden Ergänzung des bestehenden Vertrages. Der Kunde ist gegenüber der Swisscom verantwortlich, dass die Bestellungen im Dashboard durch ihn oder durch eine von ihm ermächtigte Person vorgenommen werden.

**7.2 Kündigungsfristen und Mindestbezugsdauer**  
Die Business Network Solutions Optionen haben keine Mindestbezugsdauern. Im Dashboard bestellte Optionen müssen vom Kunden selbständig im Dashboard gekündigt werden. Swisscom kann ihrerseits für allfällige Kündigungen auch andere Kanäle einsetzen. Die Kündigung des vorausgesetzten Business Internet Services aus Smart Business Connect bewirkt automatisch den Wegfall sämtlich verbundener Optionen. Die Kündigung von Managed Networks bewirkt automatisch den Wegfall sämtlicher Optionen am entsprechenden Standort.

Am Hauptstandort kann Managed Networks erst gekündigt werden, wenn an allen anderen Standorten des Verbunds sämtliche Optionen gekündigt wurden. Mit der Kündigung einer Option werden automatisch sämtliche damit verbundenen Konfigurationen gelöscht. Die Konfigurationen können nicht gespeichert werden.

### 8. Änderung und Einstellung

Die Änderungen und die Einstellung von Business Network Solutions bzw. einzelner Optionen richten sich nach den AGB und den Besonderen Bedingungen.

Oktober 2022