Schedule 11 – Avaya IX Hosted Telephony

Commencement date for provision of the Supplies

The date on which the Supplies become available for use by the Customer (regardless of whether or not they are actually used on that date), as specified in the first monthly invoice relating to the Supplies.

Description of the Supplies

The provision of Avaya IX Hosted Telephony services described in this Schedule, as specified in the Order Form.

Prices payable for the Supplies

As set out in the Order Form.

Service Level Agreements (SLAs)

A. Priority levels

The following SLA's will apply to issue resolution provided that the issue falls within the Support Demarcation Boundary as defined below.

(a) Priority 1, Critical Outage

Problems that severely affect call processing service, traffic and require immediate corrective action (24x7) for example:

- 100% of users cannot access the Services;
- 100% of users cannot connect to voice servers;
- No inbound calls can be placed into the system
- No outbound calls can be made from the system.

(b) Priority 2, Major Impact

Problems that cause conditions that significantly affect system operation, maintenance, and administration and require immediate attention. The urgency is less than in critical situations because of a lesser effect on system performance, for example:

- There are call processing issues with a majority group of users (>50% of users);
- The system performance is degraded;
- Administration of service is degraded;
- There is no reasonable workaround.

(c) Priority 3, Minor Impact

Problems which do not significantly impair the functioning of the system and do not significantly affect service to customers, for example:

- Problem is non-critical or not service affecting;
- There is a reasonable workaround;
- Usability issue, documentation problem.

B. Priority response time frames definitions

B1. The priority response time frame definitions applicable to the SLAs are as follows:

Response: the time from creation of a ticket until contacted by Connexus or its Relevant Subcontractor.

Resolution: the time from creation of a ticket until Connexus or its Relevant Subcontractor have a full fix to the issue.

Level	Category	Response	Target Fix	Measurement Period
Priority 1	Critical	1 hour	6 clock hours	24 x 7 x 365

Priority 2	Major	1 hour	8 clock hours	24 x 7 x 365
Priority 3	Minor	4 hours	3 working days	Mon - Fri 0800 : 1800

B2. Connexus or its Relevant Subcontractor shall use reasonable endeavours to provide a solution within the above target timeframes. For Priority 1, Critical Outage and Priority 2, Major Impact issues, Connexus or its Relevant Subcontractor will aim to provide a temporary solution to temporarily fix the fault with the Service while a permanent solution is developed.

B3. Priority 1 issues may be downgraded to Priority 2, and Priority 2 issues may be downgraded to Priority 3, following the application of a temporary solution.

B4. To meet these goals, at the request of Connexus or its Relevant Subcontractor the Customer shall ensure that its personnel are on site and that remote access to the Service, or affected product or system is available to allow remote diagnostics and maintenance.

B5. The Service Levels shall only apply to faults traced to Connexus's or its Relevant Subcontractor's Service platform and not to Customer CPE and Customer network connectivity related faults.

B6. It is technically impracticable to provide a fault free Service and we do not undertake to do so.

C. Incident / fault reporting

C1. To assist Connexus in meeting the service levels detailed in paragraph 14 above, when reporting an issue, the Customer shall provide Connexus with:

(a) the date and time at which the problem occurred;
(b) the Service which the problem affected;
(c) the impact of the problem on the Service including a detailed description of the issue, including:
  i. the components involved, and;
  ii. the activity ID involved in the issue, and;
  iii. any other information that Connexus may reasonably require.

C2. Following receipt of each new Incident, Connexus will allocate a unique Case Reference Number by the Connexus fault management system. The Customer and Connexus, at the time of making the incident / fault report, shall agree the priority level of the incident in accordance with the criteria set out in section B of this Schedule. Once opened, a support case will remain open until the incident has been resolved.

D. Incident resolution targets

D1. Connexus shall use reasonable endeavours to resolve an incident within the timeframes defined in section B of this schedule. Such service is available 24 x 7 x 365 days per year for Priority 1 and Priority 2 incidents.

D2. Repair times for non-Service affecting faults shall be agreed on a case-by-case basis. No Service Credits shall be payable for failure to repair non-Service affecting failures within the target repair time specified above.

E. Service availability targets and levels

E1. The Service Availability Target (defined below) relates to the ability of the active Avaya Hosted instance to be operational and reachable by an administrator over the management network, as measured and determined by Connexus.

Service	**Monthly Availability Service Level**	**Service level triggering Service Credits**	**Service level triggering Service Credits**	**Service level triggering Service Credits**
		1st trigger	**2nd trigger**	**3rd trigger**
Avaya Hosted	99.95%	<99.95%	<98.0%	<95.0%

Service Level triggering Service Credits	**The Service Credit as a percentage of the recurring monthly Charges for the affected Service shall be:**
1st trigger	10%
2nd trigger	30%
3rd trigger	50%

E2. Downtime or unavailability relating to the following incidents shall not be treated as a period of unavailability in the Avaya Hosted availability calculation, and the Avaya Hosted and

associated infrastructure and Services shall be deemed to be available during any periods of downtime caused by any of the following:

(a) any matter beyond Connexus's reasonable control;
(b) Scheduled or Emergency Maintenance;
(c) any Service-affecting fault that is not classified by Connexus as a loss of Service;
(d) the public internet (including without limitation any unavailability of the public internet);
(e) the Customer requires an ancillary product;
(f) works carried out by anyone other than Connexus;
(g) failure by the Customer to provide prompt assistance and information, as requested by Connexus;
(h) any incident that is raised by the Customer that is subject to inaccurate or incomplete information;
(i) failure by the Customer to respond to an enquiry from Connexus or any third party acting on its behalf which delays, hinders or prevents Connexus from performing its obligations;
(j) unavailability caused by a WAN or Internet service;
(k) incidents, delays and failures by Connexus to meet any Service Levels which are caused by denial of service attacks.

F. Service Credits

F1. Except as otherwise provided in this Schedule, Service Credits are applied as follows:

Failure to meet the Service Availability target: If Connexus fails to achieve the Service Availability target set out in section E above at any Site in any calendar month the Customer may claim Service Credits for the affected Service.

F2. To claim a Service Credit, the following must be submitted to Connexus within 30 days from the date upon which the relevant Incident first occurred:

(a) The Connexus support case reference;
(b) The date and time of the first contact with Connexus;
(c) Sufficient evidence and information to describe and demonstrate to Connexus's satisfaction (acting reasonably) that an Incident has occurred and that such Incident was not caused by the Customer or End User, or any of the causes referred to in paragraph 0 of this Schedule; and
(d) A request for the applicable Service Credit.

F3. If the Customer fails to submit the above information and request to Connexus within such 30 day period, the Customer shall be deemed to have irrevocably waived its right to any Service Credit that would otherwise have been payable in respect of that Incident.

F4. Service Credits can be claimed as discounts on the monthly charge. Note that for calculation purposes, a month is 43800 minutes long. Where there is no recurring monthly Charge, Service Credits are calculated based on the method outlined above.

G. Exclusions

G1. In all cases, any periods during which Scheduled Maintenance and/or Emergency Maintenance is being carried out shall be excluded from any Service Level measurement periods.

G2. Incidents, delays and failures by Connexus to meet any Service Levels which are caused by denial of service attacks shall also be excluded from any Service Level measurement period.

H. Aggregate Service Credit cap

H1. Notwithstanding any other term of this Agreement, in no event shall the Service Credits payable by Connexus in respect of a Service in any month exceed 100% of the recurring monthly Charges payable by the Customer in respect of that Service in that month.

Software licences

None.

Special Conditions

1. Definitions

The following definitions apply in this Schedule:

Avaya IX Hosted Telephony: Avaya Hosted Telephony Service.

Customer Order: an order for the supply of the Service and / or (where applicable) Equipment and / or Service Equipment.

Customer Order Variation: any variation to any Customer Order, including changes to any Service option, varying or adding to the Service or (where applicable) the supply of any additional or replacement Equipment and / or Service Equipment.

Relevant Subcontractor: the Subcontractor from whom Connexus is procuring and reselling the Service.

Service: the Supplies more particularly described in this Schedule and the Order Form.

Support Demarcation Boundary: Connexus, as part of this Service, is not responsible for:

1.1.1. PC or server hardware, operations systems or third party software, whether belonging to the Customer or made available to the Customer by a third party;
1.1.2. the Customer's site network configuration;
1.1.3. solution administration and configuration including but not limited to creating / maintaining campaigns, users, groups, routing strategies;
1.1.4. dialler management and configuration;
1.1.5. the Customer's workstation software replacement, installation or modifications;
1.1.6. access to third party client portals or software;
1.1.7. software outside the Service Demarcation Boundary including but not limited to operating systems, virus scanners, backup tools etc.

2. Orders for Service

2.1. Customer Orders and Customer Order Variations shall be binding on acceptance by Connexus.

2.2. Connexus agrees to set up the Service within reasonable timescales, subject to any timescales of the Relevant Subcontractor. All timescales and any provisional or proposed activation dates are estimates only.

2.3. Service will commence on the activation date notified by Connexus, following completion of any required set-up and installation work.

2.4. Connexus reserves the right to revoke its acceptance of any Customer Order or Customer Order Variation, if for any reason an Avaya Hosted system cannot be provided to any relevant Customer premises having regard to any geographic, practical or technical issues arising, including with respect to such premises or any local exchange. This may not be discovered until the last minute when an attempt is made to set up the Avaya Hosted system.

2.5. Property and title to Connexus equipment and all Service Equipment installed at the Customer's or a third party's site for the provision of the Service remains with Connexus and the Customer shall apply, and shall ensure that any such third parties apply, reasonable care and comply with any reasonable instructions which Connexus may issue in relation to it. Where equipment necessary for the voice service is sold to the Customer, risk shall pass to the Customer on delivery. Connexus retains property and title until it receives full payment of the due purchase price.

3. Variation to the Service

3.1. Connexus shall be entitled to make variations and additions to the Service from time to time (acting reasonably), including:

(a) to improve or add to the Services;
(b) to make changes for operational reasons where these do not have a materially adverse effect on the Service;
(c) to pass through any change made by the Relevant Subcontractor;
(d) in order to comply with any law or legal obligation (whether under common law, statute, tort or otherwise), or any change to any law or legal obligation;
(e) in order to comply with any final order, provisional order, direction, notice, specification, designation or consent made by the Office of Communications; and
(f) in order to maintain the integrity or security of the Service and / or any part of Connexus's or the Relevant Subcontractor's systems.

4. Suspension

4.1. Connexus shall be entitled to temporarily suspend and take out of use of any of the Service for operational purposes, including:

(a) updating and altering any content;
(b) replacing, maintenance, repair and upgrade of any Connexus systems and / or those of the Relevant Subcontractor;
(c) rectifying any unplanned malfunction, fault or damage;
(d) dealing with any actual or suspected security breach, virus, or attack or any misuse by any person; and
(e) taking any other action that Connexus reasonably considers necessary as a reasonable and prudent provider of the Service.

4.2. If the Service depends on a Relevant Subcontractor, then the Service may also be suspended, if the Relevant Subcontractor suspends service on similar grounds.

4.3. Subject to any requirements of any Relevant Subcontractor, Connexus will use reasonable efforts to minimise any downtime, and to carry out routine maintenance or upgrading during such times as Customer traffic is at its lowest.

4.4. In relation to any scheduled downtime, Connexus will use reasonable efforts to inform the Customer in advance.

4.5. Connexus and the Relevant Subcontractor shall be free to carry out emergency or urgent maintenance at any time to ensure the Service is continued to be supplied.

4.6. Connexus shall advise the Customer if practicable prior to the conducting of any such emergency or urgent maintenance, or at least as soon as practicable after the completion of the emergency or urgent maintenance.

5. Customer obligations

5.1. Any Customer equipment connected to or used with the Service must be connected and used in accordance with any instructions, safety and security procedures applicable to the use of the equipment. Any equipment, which is attached (directly or indirectly) to the Service must be technically compatible with the Service and approved for the purpose under any relevant legislation or telecommunications industry standards.

6. Usage conditions

6.1. Use of the Service is subject to Connexus's acceptable use policy published from time to time and the Customer must not use the Service in any way that in Connexus's reasonable opinion could or does detrimentally affect the performance of Connexus's systems or network or those of any Relevant Subcontractor, or detrimentally affect the quality of the Service to any other customers. Connexus reserves the right to take appropriate action in such circumstances.

6.2. All applicable laws and legal obligations must be complied with in connection with any use of the Service, including in relation to any activity or occupation carried out through or using the Service, and including in relation to any data, information or other materials hosted, transmitted or otherwise processed using the Service.

6.3. In particular the Service shall not be used:

(a) for or in connection with any activity which would be criminal, fraudulent or otherwise unlawful under any applicable law;
(b) to send, knowingly receive, upload, download, or process any data, information or other material which is immoral, offensive, abusive, indecent, defamatory, obscene or menacing, improper, or may cause annoyance, inconvenience or needless anxiety, or is in breach of any copyright, confidentiality obligation, or any other intellectual property right; and / or
(c) to spam or otherwise to send or procure the sending of any unsolicited advertising or promotional material, unless permitted by law, or knowingly to receive responses to any spam, unsolicited advertising or promotional material.

6.4. The Customer must be the owner of or properly licensed to use any brands, logos, and / or trade marks, and any graphics, text, sound, data, works, and other materials hosted or processed using the Service, and must ensure that Connexus and / or the Relevant Subcontractor is properly licensed to copy and reproduce such materials where Connexus's and / or the Relevant Subcontractor's systems are carrying out such actions as part of the Service.

6.5. The Customer is responsible for providing all equipment, software, systems and facilities necessary to make use of the Service. In particular the Customer shall be responsible for protecting its own computer equipment used to access the Service from viruses, spyware, or other malicious or harmful programs.

6.6. The Customer is responsible for all use and misuse of any passwords giving access to the Service. The Customer shall notify Connexus promptly of any suspect misuse or security breaches which come to its attention.

6.7. Connexus or the Relevant Subcontractor may disclose any password and encryption keys, and any information it may have gathered or which it is storing for or concerning the Customer in the provision of the Service, to comply with all applicable laws and lawful governmental requests, which may be without notice.

6.8. Connexus and the Relevant Subcontractor shall be entitled to inspect and monitor from time to time all usage being made of the Service, including communications being sent and received and data being hosted and processed, to verify compliance with these usage conditions.

6.9. Where, acting reasonably, Connexus or the Relevant Subcontractor considers that any Service is being used in breach of these usage conditions, or Connexus or the Relevant Subcontractor considers that any use being made of the Service may cause Connexus or the Relevant Subcontractor to incur any legal liability or to commit any offence, or Connexus or the Relevant Subcontractor suspects that any password is being misused, then Connexus or the Relevant Subcontractor may temporarily suspend such Service, and remove or require the Customer to remove any offending materials stored or processed using the Service, pending investigation. Connexus will endeavour to give 4 days' notice of such action, unless shorter notice or no notice is justified in the circumstances.

6.10. Connexus will only be obliged to re-instate the Service if Connexus is reasonably satisfied that no breach has occurred or will continue and that no liability will be incurred or offence will be committed by Connexus or the Relevant Subcontractor.

6.11. The Customer shall co-operate in any such investigation, and the charges for the Service will continue to be payable during such period of suspension.

6.12. The Customer shall indemnify Connexus against any liability Connexus may incur as a result of any breach of the above conditions, including in respect of content uploaded or downloaded, e-mails sent and received, and materials placed on any web space provided under the Service, and including any liability of Connexus under a like indemnity to the Relevant Subcontractor. The limitations and exclusions of liability contained in the Condition headed "Limitation of Liability" in the General Terms and Conditions do not apply to this indemnity. The liability arising out of this indemnity is limited to £1 million for any one event or series of connected events and £2 million for all events (connected or unconnected) in any period of 12 calendar months. Connexus shall have a duty to mitigate its loss in the circumstances covered by this indemnity.

7. Service description

Powered by Avaya IP Office (Containerized) overview

7.1. IP handsets that are provided as part of the Avaya service either on a rental basis or provided free of charge shall remain the property of Connexus and must be returned to Connexus at the end of the Contract, otherwise an administration fee of £50 per handset will be levied. The Customer can continue to use the handsets whilst they are contracted / paying for the Service. If the Customer has purchased the handsets outright then they own the equipment, and the provisions of this clause do not apply.

7.2. Powered by Avaya IP Office (Containerized) leverages container technologies and provides IP Office telephony and collaborative Unified Communications (UC) capabilities. Powered by Avaya IP Office (Containerized) leverages Kubernetes for container orchestration and management. Google Cloud Platform provides persistent data, internal and external networking, and other infrastructure, so the deployment does not require any additional servers or networking infrastructure.

7.3. Virtual instances are controlled by Kubernetes and monitored by Stackdriver. Google Cloud Platform provides the persistent data, internal and external networking, and other infrastructure.

7.4. With Powered by Avaya IP Office (Containerized), in addition to providing hosting services in the Google Cloud Platform, the solution also provides the following:

(a) Resiliency and HA setup. Google resiliency options are supported;
(b) Continuous around-the-clock monitoring;
(c) Outage management and recovery;
(d) Backup, restore, and disaster recovery;

(e) Software availability and registry management;
(f) Cluster upgrades and security patches;
(g) Vulnerability threat management.

7.5. *Powered by Avaya IP Office (Containerized) specifications*. The Powered by Avaya IP Office (Containerized) solution supports the following:

- Up to 400 users or extensions on a single virtual call server with up to 60 voice mail channels.
- Depending on the number of users in the initial order, one of the following profiles can be assigned:
  - Profile S1: 60 users maximum
  - Profile S2: 200 users maximum
  - Profile S3: 400 users maximum.

The following table summarises the capacities for different profiles:

Feature	**Profile S1**	**Profile S2**	**Profile S3**	**Notes**
Users				
Maximum solution users	60	200	400	
Maximum users per Customer	60	200	400	
Extensions				
Maximum normal extensions per Customer	60	200	400	All TLS
Maximum simultaneous extensions per Customer	60	200	400	This applies to Avaya Equinox®or Avaya Communicator for Web
Total extensions	120	400	800	
Maximum Remote Worker extensions	120	400	800	Infrastructure limitations could affect these numbers
Multi-site network				
Maximum nodes and locations	1	1	1	
Maximum servers	1	1	1	
Maximum expansions	0	0	0	
Trunks				
Maximum SIP trunk sessions	17	45	90	
Call processing				
Per customer call capacity (BHCC) — median	1200	4000	8000	20 calls per user per hour
Per customer call capacity (BHCC) — peak	2400	8000	16000	Over 15 minutes
Overall solution call capacity (BHCC)	1200	4000	8000	
Concurrent VoIP calls — direct media	60	200	400	Direct media is RTP or SRTP data directly between VoIP endpoints, not through IP Office
Concurrent VoIP call legs — indirect media	24	60	120	SRTP does not reduce the capacity
VCM/transcoding channels	24	60	120	SRTP does not reduce the capacity
Hunt/Presence Groups				
Maximum hunt groups .	60	200	400	Total number of hunt groups, including network and local
Maximum hunt group size	60	100	200	Collective ring mode supported at maximum users
Total hunt group members	120	400	800	Members spread over maximum hunt groups with a single hunt group not exceeding individual maximum

				size
Conferencing				
Conferencing channels	24	60	120	Both Ad-Hoc and Meet Me conferencing
Maximum conferences	8	20	40	
Maximum conference size	24	60	120	
Messaging				
Mailboxes	121	401	801	User, hunt group, and system recording mailboxes, per solution
Maximum voice mail and Auto Attendant channels	10	30	60	Common resource used for voice mail, recordings, and announcements
Maximum voice mail duration, in seconds	3600	3600	3600	Common resource used for voice mail, recordings, and announcements
Message store capacity, in hours	121	401	801	Common message and call recording storage
Single mailbox maximum capacity, in minutes	60	60	60	Combined voice mail and call recording time
Attendants				
Maximum Audio Attendants	40	40	40	
Maximum Voice mail and Auto Attendant channels	10	30	60	Common resource used for voice mail, recordings, and announcements
Call recording				
Maximum customer recording channels	8	20	40	Common resource used for voice mail, recordings, and announcements One recording channel takes three conference channels and two indirect call legs
Maximum call recording rate, BHCC	160	400	800	Normal distribution is 20 calls per channel per hour. Peak rate is 40 calls per channel per hour over 15 minutes
Maximum recording to email length, in minutes	40	40	40	20 MB size limit
Maximum recording to mailbox length, in minutes	60	60	60	
Total mailbox call recording capacity, in hours	121	401	801	Common message and call recording storage
Maximum recording to Voice Recording Library (VRL) length, in minutes	300	300	300	
Total VRL call recording capacity, in hours	25,000	25,000	25,000	
Maximum stored VRL calls	150,000	150,000	150,000	
Maximum VRL retention period, in days	365	365	365	
Maximum VRL client sessions	5	5	5	Concurrent clients with VRL activities
Maximum VRL playback/export sessions	2	2	2	Concurrent clients exporting or playing VRL
Maximum exported VRL files	50	50	50	Maximum VRL recording in one export archive
Productivity				
Active UC clients	60	200	400	This applies to Avaya Equinox® or Avaya

				Communicator for Web
SoftConsole active instances	4	10	20	
Resilience				
Maximum single phone failover time in minutes	3	3	3	
Maximum complete customer pod failover time, zonal failure, in minutes	3	3	3	
Directory				
Call logs per user	60	60	60	Last 60 retained
Networking				
HTTP and HTTPS phone server clients	120	400	800	
Start-up and availability				
Phone service availability after restart	60 within 2 minutes	60 within 2 minutes	60 within 2 minutes	
Music on hold				
Music on hold sources	4	10	20	

8. Security considerations

8.1. *Passwords*. Powered by Avaya IP Office (Containerized) does not use common default passwords. All passwords are complex and unique. Extension passwords or PINs are used for H.323 and SIP endpoints.

8.2. *Client software and firmware*. All applications are self-contained and are updated automatically, so the Customer does not need to download the latest versions. This also prevents version mismatches between applications.

8.3. *Default security settings.* By default, Powered by Avaya IP Office (Containerized) uses TLS 1.2 and SRTP. SIP-TCP and RTP are only used for legacy SIP trunks. Trusted certificates are not used. All phones are locked to the Customer instance using a unique telephony certificate.

8.4. *Administrator accounts.* Powered by Avaya IP Office (Containerized) uses multi-tier administration. For security purposes, each role can access a certain subset of administration features. All IP Office administrator accounts are created on system start-up with unique passwords. These passwords must be reset when the user logs in for the first time.

8.5. *Certificates.* Powered by Avaya IP Office (Containerized) does not require certificate administration. Each cluster has a common Certificate Agent Service (CAS) component, which can automatically request certificates from a public Certificate Authority (CA) using the ACME protocol. The Let's Encrypt CA provides a fully trusted free certificate service. Each IP Office or COM obtains its certificate on start-up, and automatically renews it 14 days before expiration.

8.6. *Google Cloud Platform security.* Powered by Avaya IP Office (Containerized) leverages Google Cloud Platform security features, including the following:

8.6.1. Kubernetes Engine role-based access control, which allows greater control over the cluster and its components.
8.6.2. Data center physical security.
8.6.3. Management of services using a secured global API gateway infrastructure.
8.6.4. Data disposal when the system is retired.
8.6.5. Vulnerability patches are installed on nodes automatically.
8.6.6. Role-based access control for service and user accounts.
8.6.7. Full audit trail. Stackdriver is used for central audit trails and security alarms.

8.7. *Kubernetes environment.* The following key security measures are available for the Kubernetes environment:

8.7.1. All pods use TLS and an internal cluster CA.
8.7.2. All sensitive data, such as customer configuration, call logs, and backups, are encrypted to a unique customer key.
8.7.3. Node hardware and base OS are hardened.

For more information about Google Cloud security, see https://cloud.google.com/security/.

8.8. *VoIP security.* Powered by Avaya IP Office (Containerized) does not support Avaya SBCE within the hosting environment. A combination of the hosting environment and enhanced IP

Office capabilities provide a comprehensive set of security features, which include the following:

8.8.1. IP, ICMP, and TCP level attack protection from DoS, DDoS, port scan, and so on.
8.8.2. Extensive SIP, H.323, and HTTP brute force resistance, including automatic source IP blacklisting.
8.8.3. Editable SIP and HTTP user agent whitelist and blacklist with active defaults.
8.8.4. Firewall capabilities, including explicit ingress and egress rules at the cloud public interface. No unused ports are opened.
8.8.5. Dedicated ports for VoIP signalling and media.
8.8.6. Always active SRTP, SRTCP, SIP-TLS, H.323-TLS, and HTTPS.
8.8.7. Transcoding of RTP and SRTP when required by the ITSP. SRTP is prioritized over direct media.
8.8.8. Network topology hiding.
8.8.9. H.323 gatekeep and SIP registrars are automatically disabled if they are not required.
8.8.10. SIP protocol scrubber and media anomaly prevention.
8.8.11. SIP trunking locked to ITSP.
8.8.12. Toll fraud controls and alarms.

All features are enabled by default and can be modified if required.

9. Support and maintenance

9.1. The Service includes IPOSS (IP Office Support Services) upgrades and updates. The Customer will be notified of the software updates, service packs and/or firmware updates in order to schedule in.

9.2. Connexus will provide Tier 1 “first call” support, MAC work and Tier 2 “troubleshooting support” for the system including handsets/endpoints and routers (for connections from the Customer’s premises to their instance in the cloud). If further support is needed, Connexus will facilitate this with the manufacturer.

9.3. In the event of any questions (including billing-related questions) or issues related to the public telecommunications service, Connexus will provide this support.

9.4. In the event that the issue is related to any other component of the Service, including licensing and / or data center connectivity, Connexus will escalate to the appropriate supplier.

10. Provisioning / programming

10.1. Connexus performs the basic provisioning, programming, licensing and verify settings.

10.2. Customer user specific programming is also handled by Connexus. This includes user profiles, hunt groups, incoming call route, and voicemail call flows. Connexus is responsible for the programming of the endpoints at the Customer location.

11. Carrier services and additional options

11.1. Connexus does not require use of specific carrier services as part of its offering therefore, the carrier services component is an optional component of the Service.