Schedule 12 – Horizon 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 Horizon 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 SLAs 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 Service;
- 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 following expressions have the following meanings for the purposes of the SLAs:

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

Resolution: the time from the 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 Connexus does not undertake to do so.

C. Incident / fault reporting

C1. To assist Connexus in meeting the service levels detailed in section B 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 above. 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 above. 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 Horizon 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 levels triggering service credits**	**Service levels triggering service credits**	**Service levels triggering service credits**
		1st Trigger	**2nd Trigger**	**3rd Trigger**
Horizon 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 Horizon availability calculation, and the Horizon and associated infrastructure and Service 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 B1 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 section E.2 above; 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 the Contract, 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:

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 a 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.

Horizon: the Horizon hosted telephony service.

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

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

Support Demarcation Boundary: the following parts of the infrastructure that the Service relies on for which Connexus is not responsible:

- PC and server hardware, operations systems or third party software, whether belonging to the Customer or made available to the Customer by a third party;
- the Customer's site network configuration;
- solution administration and configuration relating to the Service, including (but not limited to) creating, maintaining and / or removing campaigns, users, groups, and routing strategies;
- dialler management and configuration;
- the Customer's workstation software replacement, installation or modification;
- access to third party client portals or software;
- 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 The 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 a Horizon 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 Horizon.

2.5 Property and title to Connexus Equipment and all Service Equipment installed at the Customer's or third party's site for the provision of the Service remains with Connexus and the Customer shall apply, and shall ensure 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 Service;
(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 any 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 or CPE 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 trademarks, 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 suspected 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, emails 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.

Service description

1. Introduction

Horizon overview

1.1 Horizon is a complete communications service for business that provides an extensive range

of fixed and mobile telephony capabilities through easy to use web and mobile interfaces. The Service allows the Customer's administrator to easily manage the Customer's business telephony environment whilst enabling its employees to maximize their productivity.

1.2 Horizon is provided using Polycom handsets, providing high standards of interoperability and features.

1.3 IP handsets that are provided as part of the 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 the Customer owns them and the provisions of this paragraph 1.3 do not apply.

1.4 The Service offers a range of features and an emphasis on control and administration through the web that takes the burden away from the Customer's IT team. The Customer's administrator can quickly configure the system according to the Customer's changing requirements, whilst its employees can manage calls easily and effectively through additional services such as desktop and mobile client software.

1.5 At the heart of the Horizon product and combined seamlessly with the Gamma IP network is the world's leading call controller platform from Broadsoft. Supporting millions of business users worldwide with the broadest feature set and sole focus on delivering the richest user experience in Unified Communications, Horizon has a cutting edge roadmap to ensure all of the Customer's user requirements are met both now and in the future.

1.6 Integrator is a powerful piece of software that allows a user to control the Horizon Service from their desktop without having to log in to their Horizon portal or navigate through phone menus. In addition, the software integrates with a user's Outlook program making contacts easily accessible and dial-able from Outlook and the desktop. Accessing key features and settings becomes very quick and easy, and finding and dialling contacts very fast, helping users to work more efficiently and be more productive.

1.7 Telephony presence (with Click to Dial) is also provided for up to 20 work colleagues, definable by each user. Furthermore, for those Customers who use Microsoft Lync ®, they will enjoy the benefit provided by the integration of Horizon's phone status with a user's Lync status (on a call or DND).

Key features provided are:

- Click to Dial from Outlook ®;
- Screen popping from Outlook ® contacts and Horizon Company Directory;
- Click to Dial from web pages;
- In-call control features – hang up, hold, deflect, consult and transfer;
- Desktop feature control – Do Not Disturb and Forward All Calls;
- Desktop Address with Click to Dial (searches Horizon Company Directory and Outlook Contacts);
- Desktop Call History;
- Desktop Recent Call Search;
- Telephony Presence (with Click to Dial);
- Integration with MS Lync ® status (on a call or DND) Integrator CRM.

Integrator CRM provides the full functionality and associated benefits of Integrator, as well as providing integration CRM systems detailed below, and features such as desktop contacts searching.

2. Fraud Management System (FMS)

2.1 The Fraud Management System (**FMS**) feature allows Horizon systems to be monitored by Connexus and automatically bar Horizon Companies based on a user defined monetary threshold.

Horizon customers do not need to have a PBX on-site as they can access Gamma's systems via secure portals, store their data behind Connexus's supplier's firewalls, and receive regular updates to their system. However, avenues still exist that may allow a phone system to be hacked or abused, be that from an outside hacker or an employee of the Customer. The automatic barring feature reinforces the fraud management credentials of Horizon and the security of the Horizon product.

2.2 The system monitors the spend per Customer by aggregating call charges CDRs which have been matched and rated by Connexus's billing system and allocating them to timeslots. The cumulative total from the notional start time (i.e when the FMS was started) will be monitored. When the total reaches the warning threshold (typically configured at 70% of maximum

spend), the system will generate a warning email to Connexus.

2.3 Customers can then investigate the call charges with Connexus or request a raise in the spend limit. If no alternative action is taken, the system will continue to monitor the spend until it breaches either the 24 hour tracking threshold, at which point a 'Restrict Service' operation will be triggered automatically and no further outbound calls will be possible. The system will automatically generate a further email to Connexus detailing the fact that the Customer has breached its limit. The email will also detail the current spend before call barring became effective, along with a summary of the most recent call records.

2.4 Once the Customer has breached its limit and call barring has been applied, it will remain in this state until the call barring is removed by Connexus.

Note 1: Calls to the Emergency Services will be unaffected.
Note 2: The operational requirements including scheduled polling, mediation and activation logic mean that the call barring can take up to an hour to take effect. The final spend may therefore overrun the configured spend limit; a fact that should be 'factored in' when setting individual spend limits.
Note 3: The call charge aggregation is reset after a barring event is triggered. Any call charges landing after the call barring has been applied will be counted towards the new aggregation, despite potentially being made prior to the barring event.
Note 4: All calls originating from the endpoint will be included in the aggregated spend. It is expected that the total value of the calls will be higher than this email suggests because further calls are likely to be processing at the point the barring is triggered.

2.5 *Aggregation method*. As and when the FMS alerting system becomes aware of calls being made it aggregates the value of the calls from the Horizon system into hourly chunks.

2.6 After a call is completed and loaded into the system, it asks itself the following questions:

1. Does the total value of the last 24 chunks (including the current one) now exceed the warning threshold? In which case an email alert is sent to Connexus.
Or
2. Does that value now exceed the threshold for barring? In which case the endpoint is barred and a notification sent by email to Connexus.

2.7 It takes time for the system to become aware of calls being made. For this reason the final cost of the traffic may be in excess of the barring threshold.

2.8 At the point barring is removed, the value of the previous 24 hourly chunks is re-set to zero.

2.9 This is easier to explain using an example:

- Consider a new Horizon Customer that has quickly started making lots of expensive calls. The Customer is set up with fraud management enabled at time zero, with an automatic barring threshold of £500, and an alert threshold of 70% of this. Aggregation begins straightaway.

- After 19 hours the user, who has been making calls consistently over the period, triggers an alert to Connexus. This warns Connexus of the usage and that, if no action is taken, the Customer's Horizon system may get barred.

- If Connexus and the Customer do not agree to edit the barring thresholds, and the user has continued to make calls, for 29 hours the Horizon system is barred.

3. Security

3.1 The Horizon application is fully patched and recommendations and best practice guides related to security are fully implemented. Security alerts are assessed immediately and, after full testing within the lab environment, deployed via staging and production systems.

3.2 Protection is furnished by geographically distributed resilient components to ensure that impact on one element does not jeopardise protection as a whole.

3.3 Gamma supply a range of handsets which are configured to employ encrypted communications to combat 'man in the middle' exploits during installation and provisioning. Once in service, provisioning and management remain fully encrypted. IP handset provisioning is also password protected, MAC address authenticated and user agent screened. Soft client provisioning is encrypted and password protected. Integrator and the thin clients (Receptionist & Call Centre) are HTTPS and password protected.

3.4 Router and Firewall configuration is locally locked down and sensitive configuration data not accessible from the device itself. All adds / moves / changes must be made via secure Portals

over encrypted links. Portal access is closely monitored and passwords subject to minimum security standards and regularly renewed.

4. Support and maintenance

4.1 This service includes Horizon upgrades and updates. The Customer will be notified of the software updates, service packs and / or firmware updates in order to schedule in.

4.2 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.

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

4.4 In the event 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.

5. Provisioning / Programming

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

5.2 The 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.

6. Carrier services and additional options

6.1 Connexus will use the Gamma network. The Gamma network is one of the UK’s largest Tier 1 providers of voice and data services, switching in excess of 800 million minutes per month over Connexus’s soft switch infrastructure. Connexus’s Next Generation architecture, which interconnects to BT at 650 local exchanges, has been specifically designed to:

- Support the end to end automation of Customer transactions between Connexus’s Portal and Network platforms;
- Facilitate the rapid development and deployment of new product functionality;
- Ensure very high levels of system availability through multiple layers of technical and geographic resilience.