G-CLOUD 15 FRAMEWORK

SERVICE DEFINITION

Unified Communications platform and services Proposal

ISSUE 3
20th January 2026

Table of Contents

Table of Contents 2
1 SERVICE OVERVIEW & SOLUTION 3
2 INFORMATION ASSURANCE 5
3 BACKUP/RESTORE AND DISASTER RECOVERY PROVISION 5
4 ON-BOARDING AND OFF-BOARDING PROCESSES 5
4.1 On-Boarding 5
4.2 Off-Boarding 6
5 SECURITY 6
6 SERVICE MANAGEMENT DETAILS 6
6.1 Technical Boundary 6
6.2 Support Boundary 6
6.3 User Authorization and Roles 7
6.4 General Support details 7
7 SERVICE CONSTRAINTS 8
7.1 Planned Maintenance 8
7.2 Emergency Maintenance 8
8 SERVICE LEVELS 8
8.1 Award of Service Credits: 9
8.2 Payment of Service Credits: 9
9 TRAINING 9
10 ORDERING & INVOICING PROCESS 9
11 TERMINATION TERMS 9
12 DATA EXTRACTION /REMOVAL CRITERIA 9
13 DATA PROCESSING AND STORAGE LOCATION(S) 10
14 DATA RESTORATION / SERVICE MIGRATION 10
15 CUSTOMER RESPONSIBILITIES 10
16 TECHNICAL REQUIREMENTS 10
17 DETAILS OF ANY TRIAL SERVICE AVAILABLE 10
18 ICT Greening Policy Compliance 10
19 ICT Strategy Policy Compliance 10
22 Service Pricing 11
23 About your company and services 11
23 Appendix 1: GCLOUD SECURITY GUIDANCE SUMMARY 12

1 SERVICE OVERVIEW & SOLUTION

Our mission is to make technology easy and enjoyable, so our integrated range of Telephony, Contact Management & Unified Communications solutions streamline communication between colleagues and clients. Whether on or off site, they will ensure your team can do their job and help ensure service users have a straightforward, secure and consistently high level of customer experience.

Consideration as to the adoption of Cloud Telephony Services especially important as BT Openreach move to stop sell legacy ISDN & PSTN services, ahead of their planned network switch-off by 2025.

CLOUD PBX

A fully featured telephony solution suitable for all user types; benefit from a straightforward, flexible service with calls routed over the internet. This allows users to work from any location or device, while also removing the cost of legacy ISDN & PSTN phone lines and maintenance of old systems.

With loads of useful call handling features for both administrators and end users, including reporting and analytics, it is an easy way to manage calls and set policies without users being restricted to a single device or location.

Note: Internet connectivity can be provided by Windsor ensuring end to end management and call quality, or we will assess your existing services to ensure suitability. Services can also be accessed from most home and public WiFi connections, perfect for volunteers or a mobile workforce.

INBOUND CALL MANAGEMENT

From simple memorable phone numbers, to a fully featured contact centre solution; take control with advanced call management features. With the ability to dynamically manage call flows, analytics, call recording, disaster recovery and so much more, you will have access to a wealth of intelligent contact management features to have full control and visibility over your incoming calls.

Services are provided per account of telephone number, with minute bundles designed to suit your business, thus avoid the often-spiralling cost of some contact centre solutions where features are built into premium licences for individual agents.

UNIFIED COMMS

Bring all elements of communication into one place; integrate your productivity and collaboration tools including email, with presence, messaging, conferencing, video, desktop sharing, mobile and more to allow your team to be more productive.

Microsoft Teams is the world's leading collaboration service with the highest levels of user adoption, this is enhanced by our integration services that link your communications and IT together to become one seamless user experience.

SIP TRUNKING

Route calls directly to Microsoft 365, or help extend the life of existing on-premise set ups; with great value calls, enhanced management and disaster recovery features this delivers telephony over your internet connection.

Often bridging the gap between a full cloud telephony solution and existing services, this can be a great way to move to VoIP, avoid high call charges and remove legacy ISDN & PSTN lines until you are ready for the full migration to a cloud environment.

MOBILE

Ensure colleagues are connected on the go; business focused mobile plans that give you the call time and data that you need together with organisation wide control and visibility.

2 INFORMATION ASSURANCE

Information assurance and governance processes have been adopted to ensure the services are suitable for use at IL1 & IL2. Annual penetration testing provides assurance that your data and services are in safe hands.

3 BACKUP/RESTORE AND DISASTER RECOVERY PROVISION

Backup, restore and disaster recovery provisions are included by design, including a cloud first architecture that features multiple availability zones for all internal and customer applications.

4 ON-BOARDING AND OFF-BOARDING PROCESSES

4.1 On-Boarding

Setting the foundations for customer success is at the heart of the on-boarding process, this includes ensuring a great end user experience and high-levels of adoption. Our process has three clear tracks:

- **On-boarding your organisation;** this welcomes you as a new customer to Windsor and sets up the relationship. We ensure clear expectations are set with project owners to make sure all contracts and service level agreements are in place, a contact plan and is established and that you are clear on how to reach us should you ever need help and support. We will also set

up and train administrators on our portals and that billing, payment and service reporting processes are all set up.

- **Implementing your solutions;** we will agree an implementation plan and set out our regular KCI (keeping customer informed) cadence. All solutions will be overseen by a member of our account and customer success team and depending on the scale and complexity either a provisioning coordinator or dedicated project manager will be also be on hand to ensure delivery to time, budget and quality. As well as establishing our own services and work with our technology partners (such as carriers for the delivery of new infrastructure, or vendors for any required hardware), but with your consent can support managing your legacy suppliers during any porting or migration process.
- **Adopting your services;** our customer success and training team will ensure both the admin and end user profiles are correctly set up, so everyone can take full advantage of the service. This includes comprehensive user guides but can also incorporate 'train the trainer' or direct user training and support as needed, both virtually and on-site.

4.2 Off-Boarding

We hope to have a long and happy relationship but being a customer for many years should not mean keeping the same service. Flexibility is at the heart of true cloud services, so we aim to ensure you are always able to access the most recent possible version of our services and support movement between types of licence in agreements where we can.

In the event that the solution includes the provision of customer premise equipment for which we retain title, you may be asked to arrange a mutually convenient time, during business hours, for us to arrange its collection.

Reasonable transition assistance will be provided based on time incurred per the SFIA rate card.

After the expiry of the agreement, data and information will continue to be held and processed in line with our then current Privacy and GDPR policies.

5 SECURITY

Our products and services, together with our internal and external systems and processes follow the principle of being secure by design. This is a requirement we extend to all our technology partners. We are committed to maintaining Cyber Security Plus accreditation and following the essential GCloud Security Principles contained within Appendix 1, together with any other relevant solution specific measures. Security is an executive responsibility on which the COO reports to the board of directors on a monthly basis.

6 SERVICE MANAGEMENT DETAILS

6.1 Technical Boundary

Technical boundaries are defined on a product or service specific basis, but will typically include the provision of all software, core services, portals and where applicable Customer Premise Equipment.

6.2 Support Boundary

Support boundaries are defined on a core systems, service or end user basis. Windsor will always ensure full accountability for the matters relating to core systems which will be proactively managed. Support will be offered to customers' administrators in relation to all services in line with the product and solution specific requirements to ensure they can be used as intended. End user support will typically only be offered where this has been specifically agreed as part of the scope.

6.3 User Authorization and Roles

We offer a three core levels of permissions-based access and support:

- **Account Authority:** This level can enter commitments on behalf of the customers and approve moves, adds and changes, including adding other Account Authorities.
- **Account Administrator:** This level will be able to add and remove users and specific features, including changing other users' settings at an individual or departmental level.
- **End User:** This level will have access to only to services specifically assigned for their use and the ability to utilise functions used in their day to day working.

We utilise encrypted passwords and offer single sign on with the ability to offer two-factor authorisation.

6.4 General Support details

We actively track customer satisfaction using and NPS survey. We share our roadmap with our customers and actively encourage product improvement input. All clients are allocated a dedicated account manager who can be accessed directly during working hours via phone, email or online chat, as well as a dedicated emergency helpline that can be called 24 hours a day, 365 days a year.

Windsor Telecom are here when you need us:

Customer Services Enquires	Telephone 0333 123 8080
(Monday to Friday 9am to 5pm):	Email: service@windsor-telecom.co.uk
	Webchat: www.windsor-telecom.co.uk
Technical Support Enquires	Telephone 0333 123 8080
(Monday to Friday 9am to 5pm):	Email: support@windsor-telecom.co.uk

	Webchat: www.windsor-telecom.co.uk
Urgent Support	Telephone 0333 123 9090
(24x7x365):	

7 SERVICE CONSTRAINTS

7.1 Planned Maintenance

Planned maintenance is rarely customer affecting and is always only carried out following careful risk assessments. Where it is deemed that may be some risk to service this will be performed out of business hours and in the event the risk is increased beyond a notional level, customers shall be given advance warning of such maintenance. There is a status portal that customers are able to subscribe to which is fully populated.

7.2 Emergency Maintenance

Emergency maintenance is rarely required and is typically not customer affecting, in that is usually confirmed to one part of a resilient system. In the event emergency maintenance is required and this is likely to be customer affecting, the planning and risk assessment will include making provision to minimise the impact in terms of scope and duration. Where we can, advance notice will be given. . There is a status portal that customers can subscribe to which is fully populated.

8 SERVICE LEVELS

We are committed to proving a consistently excellent service, with a 100% target availability for all core systems and platforms.

In the event of service interruption, incidents will be assigned the following Priorities:

- **Priority 1 (Major Incident):** Total loss of service to a core system, or a fault causing serious business interruption to one or more customers. Escalated to COO immediately.
- **Priority 2 (Critical Incident):** Degradation of a core system, or a fault materially business impacting to one or more customers. Escalated to COO after 2 hours.
- **Priority 3 (Important Incident):** Impact to non-essential systems or partial loss of resilience, a fault affecting one or more customers, but with limited business impact. Escalated to COO after 4 hours.
- **Priority 4 (Minor Incident):** Limited impact to non-essential systems, a fault affecting one or more customers, but with little or no business impact. Escalated to COO after 8 hours.

8.1 Award of Service Credits:

Where offered, Service Credits will be based on exceeding the Maximum Time To Restore (MTTR) for the applicable service elements, as specified within the Product Terms and Customer Order (please note the MTTR will vary as they are often based on a flow down of service standards available from differing technology partners).

- MTTR exceed by up to 2 hours = 1 days rental costs
- MTTR exceed by up to 4 hours = 3 days rental costs
- MTTR exceed by up to 8 hours = 7 days rental costs
- MTTR exceed by more than 8 hours = 14 days rental costs

MTTR will be measured from the earlier of Windsor detecting the issue, or the customer reporting the same to Windsor. If applicable, any 'stop the clock time' shall not count towards the calculation.

8.2 Payment of Service Credits:

Where appliable Service Credits can be claimed by the customer and will be applied as a credit on the relevant account.

9 TRAINING

A comprehensive set of on-boarding and training materialise are available. Depending on the service and implementation plan agreed upon, full training can be provided to both systems administrators and a train the trainer approach, as well as directly to end users. This is typically delivered online, however can be included with face to face on-site training.

10 ORDERING & INVOICING PROCESS

We encourage orders via electric media, including our portals, where possible, however physical order forms can be supported if preferred. Invoicing is typically electronic via email, with back up data accessible online. Standard payment terms are 14 to 30 days via Direct Debit, with alternative arrangements by agreement.

11 TERMINATION TERMS

Should you need to leave us, please follow our off-boarding process. All our agreements can be terminated on 30-days notice, providing any minimum term has expired. Please provide notice of termination in writing, which can be submitted electronically.

12 DATA EXTRACTION /REMOVAL CRITERIA

Data is destroyed in accordance with our GDPR policy which is available on our website. Any hardware disposals are made in accordance with current guidelines, with the equipment being wiped and then disposed of in accordance with WEEE regulations.

13 DATA PROCESSING AND STORAGE LOCATION(S)

Data is stored in a cloud environment, using secure servers. Data is accessed and managed by Windsor Telecom employees on a permission-based access with users having the lowest level of access required to undertake their duties successfully. Windsor domiciles all its data in the UK.

14 DATA RESTORATION / SERVICE MIGRATION

Data is stored in a secure resilient environment and backed up appropriately. Any unplanned outages are managed as set out in point 9 above and communicated to all customers with regular updates using our status portal.

15 CUSTOMER RESPONSIBILITIES

Customer responsibilities are laid out in our standard terms and conditions.

16 TECHNICAL REQUIREMENTS

Our products are cloud based and may be accessed using a variety of media, including browsers, mobile apps and hardware.

17 DETAILS OF ANY TRIAL SERVICE AVAILABLE

Where possible we encourage customers to take both trials and our supported proof on concept as part of their process to finalise and to agree requirements. These are typically free of charge for qualifying organisations.

18 ICT Greening Policy Compliance

In additional to regulatory compliance, we are committed to supporting government Green initiatives. We aim to operate a paperless office and actively support recycling in the work environment.

19 ICT Strategy Policy Compliance

We are supportive of the government ICT strategy, including digital by default and measures to improve the availability of super-fast connectivity.

20 Service Pricing

We believe that making technology easy and enjoyable should apply as much to the commercial relationships as it does the products and services we provide.

Our pricing will always be clear and transparent, as well as tailored to your specific requirements, with any one-off and recurring fees clearly set out. Example pricing can be found within the rate cards provided, with a full quote available from our account teams.

23 About your company and services

MAKING TECHNOLOGY EASY AND ENJOYABLE

With five generations now working side by side, it can be hard for businesses to find the right way to get the best from everyone and to engage brilliantly with customers. What you need are IT and communication systems that are easy to use, yet flexible and adaptable enough to suit all your differing needs.

We focus on creating straightforward solutions that our customers enjoy using and that provide them with genuinely useful features that will make their working lives easier. Helping our customers to connect, communicate and collaborate better, in new and more intuitive ways, is what will always keep us pushing to provide great products and the accompanying service that continually make them smile.

OUR HISTORY

Windsor Telecom started out in 1999 and soon became the leading provider of memorable phone numbers and the services that helped businesses make it easy for customers to connect with them. Since then we've grown into a full-service technology partner, supporting over 6,000 businesses with their connectivity, communication and IT services needs.

OUR PASSION

We love helping customers get the most from technology, but most of all we love making them smile with both our service and our easy approach to technology and doing business together. You'll feel that from the first time we get in touch, when we listen to and understand your business challenges and most importantly if you ever need to call for help or support.

If that's the kind of relationship you want as your business evolves and grows, talk to us.

"People at work deserve the same simplicity they experience as with their tech at home. And that's what we're creating. We're growing a business here at Windsor that's focused on creating

technologies that people love using. And we're delivering it with a service that makes our customers feel special. Helping everyone get the most out of their business tech."

Pete Tomlinson | Chief Executive Officer

23 Appendix 1: GCLOUD SECURITY GUIDANCE SUMMARY

This section of the Cloud Security Guidance summarises the essential security principles to consider when evaluating cloud services, and why these may be important to your organisation. Some cloud services will fulfil all the security principles, while others only a subset.

- **Consumers** of cloud services should decide which of the principles are important, and how much (if any) assurance they require in the implementation of these principles.
- **Providers** of cloud services should consider these principles when presenting their offerings to public sector consumers. This will allow consumers to make informed choices about which services are appropriate for their needs.

The Cloud Security Principles are summarised in the table below.

Cloud Security Principle	Description	Why this is important
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit. Implementing 'Data in transit protection'
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage. Implementing 'Asset protection and resilience'
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers can not prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service. Implementing 'Separation between consumers'
4. Governance framework	The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments. Implementing 'Governance framework'
5. Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it. Implementing 'Operational security'
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service

Cloud Security Principle	Description	Why this is important
		provider personnel is increased. Implementing 'Personnel security'
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity. Implementing 'Secure development'
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles. Implementing 'Supply chain security'
9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data. Implementing 'Secure consumer management'
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur. Implementing 'Identity and authentication'
11. External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it. Implementing 'External interface protection'
12. Secure service administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data. Implementing 'Secure service administration'
13. Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales. Implementing 'Audit information provision to consumers'
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers. Implementing 'Secure use of the service by the consumer'