Claranet

Managed Public Cloud

Service Description v1.1

claranet | Make modern happen®

Contents

1. Introduction

This Service Description describes the service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and should be read in conjunction with the terms of the Customer Experience for Managed Services Document ("**CXMS**") and the Claranet Master Services Agreement ("**MSA**") set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, all terms used within this document are in accordance with the terms to be found in the CXMS and the MSA.

Claranet provides the following services as part of its Managed Public Cloud ("**Service**"). The Service components and features are set out below along with the related responsibilities for that Service component/feature.

2. Scope of Service Description

The Customer agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. Any components which are described as optional or additional in this Service Description will be chargeable at additional cost and will need to be purchased by the Customer and an Order Form or Statement of Works will need to be signed by the Customer.
Notwithstanding this, in the event Claranet completes additional services, activities and/or deliverables upon the request or at the direction of the Customer, Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed.

3. Service Overview

Claranet's Managed Public Cloud Service brings together management, backup, recovery, and monitoring of a public cloud environment, regardless of whether the cloud environment already exists or is built from scratch. Whatever the business size, the Service will ensure that the cloud environment fits to current best practices and reliably performs for the business whether in busy periods or not, scaling to the Customer's business needs.

4. Service Features

The Service supports the following features:

4.1. Standard Features

The following features are supported and included as standard:

Feature	Description
Environment	
Monitoring	Claranet will monitor the following: • Manage environment quotas and hard limits – this will ensure any managed deployments or infrastructure changes are successful. • Planned maintenance – this will ensure notification is provided of any planned infrastructure maintenance that could impact the Service. • Security configuration – this will ensure that any events relating to changing the secure configuration of the environment creates appropriate Incidents and Risks.
Security controls	Claranet will initially configure and advise on the security credentials related to the Customer's cloud subscription and relevant SAML (Security Assertion Markup Language) provider. Claranet will ensure that all data managed by Claranet are encrypted at rest. Security compliance certification remains the Customer's responsibility, but Claranet will perform the following on a reasonable endeavours' basis through: • Design, deployment and configuration of the Customer's environment using security best practices and principles; and

	• Advising the Customer on security and data compliance controls for data under the Customer's control.
Managed Operating System	

Installation, configuration and maintenance	• **Resource management**: Claranet will monitor the capacity and performance of the VM, including CPU, memory and disk utilisation, to reflect the Customer's set requirements for the applications running on that VM.
	• **OS configuration**: Claranet will configure and maintain the VM and its OS. This includes:
	  ○ Enabling/disabling specific OS features;
	  ○ Configuring system logging;
	  ○ Adding/removing additional disks and/or network devices; and
	  ○ Configuring and managing clustering.
	• **File system management**: Claranet will manage the file systems and associated disks meet the Customer's defined capacity and performance requirements of applications running on the VM. This includes:
	  ○ Increasing file system capacity;
	  ○ Growing file systems to span multiple physical devices; and
	  ○ Changing the type and/or performance of the physical devices as may be required.
	• **Management tools**: Claranet will manage the installation, configuration and maintenance of all management tools required for the operating of Claranet's services. This includes, but is not limited to, the following:
	  ○ Monitoring agents;
	  ○ Patching agents;
	  ○ Platform-specific agent software.

	• **Licensing**: Claranet will ensure the OS are licensed correctly.
	• **Network**: Claranet will configure the local network settings.
	• **Vendor Escalation**: Any OS issues that are unable to be resolved by Claranet will be escalated to the appropriate vendor on the Customer's' behalf when either:
	  ○ Customer provides the OS license, support contract and an appropriate contract details and escalation path; or
	  ○ Claranet provides the OS license and support contract.

Monitoring	Claranet will monitor the following**:**
	• CPU, memory, disk utilisation;
	• IP based up/down availability;
	• System errors and warnings;
	• Services - monitor OS specific services, including:
	  ○ Windows: windows update, firewall, event log and time;
	  ○ Linux: system, syslog, ntp.

Patching	• **Patch identification:** Claranet will perform monthly reviews to identify any patches that need to be applied to the Customer's systems. This includes any critical or security patches. • **Patch testing:** Where Customers make use of staging environments, Claranet will facilitate patching the staging environment first to allow updates to be tested to ensure they don't cause any compatibility or stability issues with the existing software before being rolled out to production environments. • **Patch deployment:** Once patches have been tested and approved, Claranet will deploy them to the production environment during a pre-agreed maintenance window. Out-of-hours work will incur additional charges and will be costed accordingly.

	• **Rollback capability:** In the event that a patch causes an Incident, Claranet has the capability to roll back the changes and restore the Customer's system to its previous state. • **Reporting:** Claranet will provide a monthly report that summarises the status of the patch management program, including any patches that were applied during the reporting period, and any outstanding patches that still need to be applied. • **Compliance:** The patch management process is designed to ensure that systems comply with relevant regulatory requirements. ○ VM patching – this will ensure that any supported VM has the latest OS security patches that are updated monthly. VM minor upgrades – this will ensure that any supported VM is updated to the latest minor version release of the OS.
Managed Platform as a Service ("PaaS")	

Installation, configuration and maintenance	• **PaaS configuration**: Claranet will configure and maintain the PaaS service. This includes:
	  ○ Enabling/disabling specific features;
	  ○ Configuring system logging;
	  ○ Increasing/Decreasing capacity.
	Licensing: Claranet will ensure what where required the PaaS services are licensed correctly where the customer has opted to bring their own existing license to the platform.

Monitoring	Claranet will monitor the following**:** • CPU, memory, disk utilisation (or equivalent) for compute-based services; • System errors and warnings; • PaaS specific metrics, including:

	○ Transactions and performance for queue-based services; ○ Success/Failure for job-based services.
Patching	Claranet will ensure that where platforms as a service support the upgrade of the underlying managed software, that the platform service is updated monthly to the latest minor version release. Claranet will ensure that any custom container images created by Claranet that are used in the deployment of containerised infrastructure, where the container is based on a Windows or Linux operating system, are updated monthly to the latest operating system security patches based upon pre-agreed automated update schedules.
Infrastructure as Code ("IaC")	
Installation, configuration and maintenance	**Templates:** • Claranet will maintain IaC using templates which are customised for the Customer and its environment. • Claranet will ensure that all templates, modules or other code provided as part of the Service remain up to date with the latest versions and remain compatible with all other tooling provided as part of the solution. • Claranet retains the intellectual property associated with the templates it produces, unless otherwise agreed with the Customer. Claranet may release these templates from time to time using an industry standard open-source licence. **Code repository:** • Claranet will ensure that all IaC managed by Claranet is stored in an appropriate source control repository and that the code is managed to Claranet's standards, including branching, tags, and releases. **Code:**

	• Claranet uses industry standard IaC tools and their associated code languages. Claranet reserves the right to change to other IaC tools from time to time. • Claranet will support existing IaC tools and code as part of the Service so long as they are compatible with Claranet's standard tool set. • Where existing code does not meet Claranet's standards, Claranet will remediate the IaC at additional cost to the Customer. **Co-management**: • Where IaC is co-managed, Claranet and the Customer must agree roles and responsibilities of which engineers will have access to make changes or review code as part of the Service. A review process must be outlined between Claranet and the Customer to ensure that any changes introduced through co-management are understood and meet Claranet's standards.
Monitoring	Claranet will monitor the following**:** • Errors and warnings generated by IaC tooling; • Variation between the code and current state of the cloud environment, due to manual changes.
Patching	Claranet will update the IaC tooling on a quarterly basis to match the latest minor version. Where this policy is met by a change in licensing or an alternative but compatible tool is introduced, Claranet will provide the Customer no less than 30 days' notice of the change.
Continuous Improvement / Continuous Deployment ("CI / CD")	
Installation, configuration and maintenance	**CI / CD infrastructure and tooling:** • Claranet will ensure that CI / CD tooling is installed and configured in order to deploy and execute the IaC code that

	is part of the Service. This will include any customisation such as plugins or integrations. • Where the CI / CD tooling requires the deployment of Operating Systems or PaaS services, for example as worker nodes, then they will be managed according to the obligations of this Service. • Claranet will support existing CI / CD tools as part of the Service, as long as they are compatible with Claranet's standard tool set. Where existing tooling does not meet Claranet's standards, Claranet will remediate the IaC at additional cost to the Customer. **CI / CD pipelines**: • Claranet will configure pipelines to test, deploy and execute the IaC code. Claranet will ensure that pipelines are configured to provide the capability of fully automated or "push button" deployments of IaC code to all supported environments.
Monitoring	Claranet will monitor: • the completion status of CI / CD pipelines; • any errors returned through running the pipelines; • the status of any runners / agents used to process the pipelines.
Patching	Claranet will ensure that its automated CI / CD tooling and corresponding plugins or extensions that are used to manage and deploy infrastructure components are updated to the latest minor versions on a quarterly basis.
Security Controls	
General	Claranet includes a suite of security controls designed to minimise the risk of security breaches and to ensure the confidentiality, integrity and availability of the Customer's data.

	Claranet will ensure that its access to the Customer environments is secure, proportional and reviewed on a quarterly basis in addition to existing joiners and leavers processes. • Virtual machine access by SSH or RDP will use named accounts accessed from secure management systems. • API access used by any tools or scripts will be linked to individual applications or named users. • All named accounts will access the environment using limited and proportional role-based access controls, agreed with the Customer. • All named accounts managed by Claranet will be subject to Claranet's standard security policies including complex passwords and multi-factor authentication. All data managed by Claranet is encrypted at rest using either platform-managed or Customer-managed keys. Claranet will make recommendations to ensure any deployed infrastructure and applications increase their security posture through encryption in transit, where appropriate.
Onboarding	The onboarding phase includes several tasks, and any additional tasks specified within the Statement of Work. Claranet will ensure that all Claranet engineers that require access to support the Customer's environment have named accounts and sufficient permissions. • Domain accounts for Windows environments – named accounts in the Customer's domain(s) within a self-managed group with local machine administrator permissions. • SSH access for Linux environments – named accounts with public keys distributed to all machines by configuration as code. • API access keys required by Claranet's tools and scripts.

	Where the Customer retains responsibility for access management, Claranet, the Customer will be required to provide all reasonable access to environment as requested by Claranet from time to time.
Financial Operations ("FinOps")	
FinOps	Claranet offers a FinOps service as a managed offering to help the Customer control their cloud spend, improve cloud cost reporting across the Customer's business and make cost optimisation recommendations with support from Certified FinOps Practitioners. Where Claranet manages the Customer's billing, and the Customer bills over £10,000 per month, the Customer is able to request the standard FinOps service to be set up. Where Claranet does not manage the Customer's billing or billed spend is less than £10,000 per month, the FinOps service will be available at additional cost. See the FinOps Service Description document for further details.
Reporting	
Reporting	Monthly patch reporting will be provided, which includes all virtual machines, containers, and other PaaS managed by Claranet that are required to be patched or already patched in the previous month. It will include an indication of the patching compliance status against each asset. An annual health report will be provided which includes a list of any platform issues which may have had an impact on the Customer's environments (with or without associated issues).
Network	
Installation, configuration and maintenance	Claranet will ensure the public cloud environment has sufficient connectivity to on-premises or other cloud environments to mee the needs of the Customer.

	Where the network infrastructure does not exist or is not sufficient, Claranet will install and configure additional network devices and connectivity at the additional cost to the Customer. Claranet will maintain any additional networking devices, including backup and patching where required according to the relevant Service Description(s).
Monitoring	Claranet will initially configure and provide ongoing monitoring of the cloud native network services and components as part of the Customer's cloud environment: • Gateway or router; • Firewall; • Network load balancing; • Application load balancing; • Domain Name System ("**DNS**") configuration; • Content Delivery Network ("**CDN**") configuration; • Distributed Denial of Service ("**DDoS**") protection configuration. Claranet will validate the initial configuration and monitor the secure private network connectivity services: • Express Route connectivity for Azure; and • Direct Connect connectivity for AWS.
SSL / TLS certificates	Claranet will initially install, configure and validate certificates purchased through Claranet or provided by the Customer.
Backup	
Security and access	Claranet requires sufficient access to all infrastructure and backup service components to manage the Customer's recovery environment.

	Claranet will restrict access to backup data and functionality using the Identity and Access Management and Role-Based Access Control platform mechanisms.
Installation, configuration and maintenance	Claranet will establish a platform-native or select third-party backup solution, where Claranet will, for supported resources, provide the following: **Platform:** • Deployment and configuration of backup service resources. • Install and configure the platform backup agent on supported Infrastructure-as-a-Service ("**IaaS**") resources. • Monitor backup platform resources and ensure sufficient capacity of the platform. **Policies:** • Backup plans. • Schedules and frequency. • Retention policies and tiering. • Immutability and soft delete. • Workload groups. • Application-consistent backups for supported workloads. • Encryption settings applied to the backup service for in-transit and at-rest scenarios using platform-managed keys. • Restrict access to backup data and functionality using the Identity and Access Management and Role-Based Access Control platform mechanisms. • For PaaS resources without native support for the platform or third-party backup service but with support for backups to native cloud storage, Claranet will configure data backups to a blob storage service for long-term retention, versioning, archival, and integration with the backup service. • Claranet will advise the Customer where no backup is required due to a logical separation between compute and

	data including but not exclusive to containers and ephemeral infrastructure. **Default Backup Policy**: While Claranet will work with the Customer to define suitable policies and configurations, where the Customer has no input or preference, Claranet will provide a set of default parameters. A daily backup of supported services to be taken in an out-of-hours window starting at 20:00 (UTC) in a single backup set. The first backup of each schedule will be a full backup, with incremental backups thereafter. Unless specified by the Customer, Claranet will adopt platform-provided soft-delete capabilities. Immutability is only implemented on request if supported by the platform. To protect data sovereignty and control costs, backup services will be configured to store backups in a single region unless platform-supported cross-region backup or retention is requested by the customer. Claranet will use the default platform capabilities for data encryption at rest and data encryption in transit. Default backup retention may be classified as either bronze, silver, or gold, with **bronze** being the default classification: • **Bronze:** Daily backups for 30 days. • **Silver:** Bronze plus weekly backups for 12 weeks. • **Gold:** Silver plus monthly backups for 12 months. Any modifications or additions to the default backup policies can be made via a ticket with the Claranet Service Desk.
Monitoring and Reports	Claranet will: • Monitor the overall backup service health; • Monitor the success status of scheduled backup and restore jobs;

	• Monitor the health of backup agents; • Provide monthly reports summarising the status of backup jobs across the service.
Patching	Claranet will: • Ensure platform backup agent patches are successful, and escalating issues to the vendor as necessary; • Regularly patch supported third-party backup solutions at the OS and application-level during a maintenance window defined as outside of the scheduled backup window; • Notify the Customer before carrying out any service-impacting maintenance.
Testing	To verify the reliability and effectiveness of the backup service, Claranet will do the following: • Following deployment, perform a functional backup and restore test of a subset of resources. These resources should be representative of a typical workload within the environment or may include the most crucial components. Claranet will work with the Customer to select suitable workloads for testing. • Perform a functional test restoration of a subset of resources once per contract year. These resources should be representative of a common workload within the environment or may include the most crucial components. Claranet will work with the Customer to select suitable workloads for testing. • Provide suitable evidence of a successful restore to the customer. Evidence may in the form of vendor-provided job reports or relevant logs from testing automation. • Work with the Customer to define testing runbooks detailing the workloads, restore sequence and evidence capture requirements.

	• Clean up test resources following successful validation.
Restore Invocation	Claranet will acknowledge a restore request with the following criteria: • A user with suitable access raises a ticket with the Claranet Service Desk. • Claranet will restore the last successful backup unless otherwise instructed by the Customer, who may request a restore from a backup that falls within the configured retention period. • The restore process may require a restart of the system, and pending system or application updates may affect system stability. • Claranet will restore the complete instance either to the original location or another specified by the Customer. Where the original and restored instance are both retained, this will consume additional platform resources and incur extra fees from the cloud provider. • Claranet will avoid overwriting existing data unless instructed otherwise by the Customer. Customers using the cloud-platform backup service will have access to self-service portals to perform restores. Where a Customer overwrites files, it accepts and acknowledges that Claranet will not be liable.
Disaster Recovery	
Deployment	Claranet will establish a platform-native or select third-party recovery solution for IaaS, and for supported resources, provide the following: **Platform:** • Deployment and configuration of recovery service resources. • Install and configure the platform recovery agent on supported IaaS resources.

- Monitor recovery platform resources and ensure sufficient capacity of the platform.
- Source and target regions should already have landing zone infrastructure deployed. Claranet can assess the suitability of the source and target regions or zones and make recommendations. Please note that remediation activities are outside the scope of this agreement.

Recovery Policies:

- Recovery point retention period.
- Application-consistent recovery points for supported workloads.
- Resource and network mapping.
- Recovery plans.
- Encryption settings applied to the backup service for in-transit and at-rest scenarios using platform-managed keys.
- Restrict access to backup data and functionality using the Identity and Access Management and Role-Based Access Control platform mechanisms.

Default Recovery Policy:

While Claranet will work with the Customer to define suitable policies and configurations, where the Customer has no input or preference, Claranet will provide a set of default parameters.

- All supported resources will be placed into a single recovery plan.
- Unless specified by the Customer, Claranet will use a like-for-like resource configuration mapping between source and target regions where applicable. For example, source and destination VMs will be configured similarly in terms of compute, memory, disk and network allocation.
- The Customer should provide a network map of the source and destination subnets; otherwise, it will be assumed that

	Claranet will use its best judgment when configuring the service. • Recovery point retention will be set to one (1) day. • Claranet will use the default platform capabilities for data encryption at rest and data encryption in transit. Any modifications or additions to the default recovery policies can be made via a ticket with the Claranet Service Desk.
Security and access	Claranet requires sufficient access to all infrastructure and recovery service components to manage the Customer's disaster recovery environment. Claranet will restrict access to recovery data and functionality using the Identity and Access Management and Role-Based Access Control platform mechanisms.
Runbooks	Claranet will work with the Customer to define runbooks which will detail the sequence and process to be followed during failover and failback, including any required testing, based upon the recovery plans defined in the recovery service. Runbooks will include clear roles and responsibilities. This includes actions for Claranet to take against supported resources, as well actions for the Customer and external suppliers to carry out. The Customer will supply contact information for key personnel and users authorised to request a failover. The runbook will provide clear criteria defining what constitutes a disaster event. The Customer is responsible for notifying Claranet of any changes to their environment which may impact the effectiveness of the process defined in the runbook. Claranet is not responsible for the recovery of business processes or services external to the supported solution.

	The Customer will have a maximum of fifteen (15) days to review and approve the runbook. If Claranet receives no response after the 15-day period, it will assume acceptance. Any amendments to the runbook will be a change and may incur additional costs.
Monitoring and reporting	To ensure a reliable recovery service, Claranet will: • Monitor the overall health of the recovery service; • Monitor the replication sync status; • Monitor the health of recovery agents and servers; • Provide regular reports summarising the status of protected workloads. Claranet will monitor the health and readiness of the supported destination recovery site. Claranet reserves the right to change its monitoring tools, methods, parameters and polling intervals over time Where necessary, Claranet will manage and escalate any incidents with the platform provider.
Capacity Management	Where necessitated by the recovery platform, Claranet will continually monitor recovery infrastructure capacity. This will include disk space, storage account limits, recovery plan limits, and compute capacity. Claranet will inform the Customer of any recommended capacity increases, indicating where these changes may incur additional platform costs.
Maintenance, updates and patching	Claranet will ensure a reliable recovery service by: • Ensuring platform recovery agent and server patches are successful and escalating issues to the vendor as necessary. • Supported third-party recovery solutions will be regularly patched at the OS and application level during a maintenance window.

	• Claranet will notify the Customer before carrying out any service-impacting maintenance. • Claranet may request a customer review of the failover runbooks.
Annual recovery testing	To verify the reliability and effectiveness of the recovery service, Claranet will: • Following deployment, Claranet will perform a functional failover test of a subset of resources. These resources should be representative of a typical workload within the environment or may include the most crucial components. Claranet will work with the Customer to select suitable workloads for testing. • Claranet will perform a functional test failover of a subset of resources once per contract year. These resources should be representative of a typical workload within the environment or may include the most crucial components. Claranet will work with the Customer to select suitable workloads for testing. • Claranet will provide suitable evidence of a successful failover to the Customer. Evidence may be in the form of vendor-provided job reports or screenshots of platform and resource interfaces, for example, a desktop screenshot of a restored IaaS virtual machine. • Claranet will use learnings from these failover tests to further refine the runbooks. • Claranet will clean up test resources following successful validation. Success criteria will be defined in the runbook. • Recovery tests will be conducted during regular business hours.
Recovery invocation	Claranet shall acknowledge a recovery request with the following criteria: • A user with suitable access and authorisation raises a ticket with the Claranet Service Desk.

- Unless otherwise specified by the Customer, Claranet will assess the primary site to determine if it is beyond remediation and warrants a failover in accordance with the disaster criteria defined in the runbook.
- Claranet will restore the last recovery point for each resource unless otherwise instructed by the Customer, who may request a recovery point that falls within the configured retention period.
- Claranet will follow the steps outlined in the runbook. This will be shared with the Customer.
- Claranet will fail back to the primary site upon request by an authorised user.
- Claranet will raise and manage issues with the platform vendor where necessary.
- Claranet will open and maintain a suitable channel of communication with the Customer.

Customers using the cloud-platform backup service will have access to self-service portals to perform failovers. In this case, Claranet will not take responsibility for the failover process.

4.2. Additional/Optional Features

The following features can be purchased on top of the standard Service and will be subject to additional charges:

Feature	Description
Additional Patching features	• Additional update categories (other than critical or security). • Major version upgrades (applies to virtual machine image patching, container patching, PaaS engine major updates). • Ensure any application frameworks including Java and .NET, installed as part of the supported machine images or PaaS services are updated monthly to the latest minor release. • Customised versions of standard container images (those not normally maintained by Claranet or the Customer and are sourced from elsewhere) needed to resolve a security issue, rather than updating to a new version of the image from the existing vendor-supplied source. This image will then need to be processed through the Change Management procedure and charged for, until a suitable vendor supplied image is available.
Additional Infrastructure as Code features	• Providing access to secure source control repositories and maintain appropriate access control for Claranet and Customer stakeholders. • Configuration management as code: maintenance of code used to manage operating system configuration and / or configuration of virtual machine images. • Co-managed code: maintain the quality and stability of IaC code maintained by both Claranet and the Customer, through code reviews of all Customer changes. • Claranet reserves the right to suspend SLAs where an issue has been caused by Customer code changes, and to charge

	for any remediation necessary as a result of Customer changes through any alternative means other than the IaC code provided.
Additional CI / CD features	• CI / CD tools build and maintain – ensure Customer requested CI / CD tools exist in the environment in order to manage IaC code deployments and that the infrastructure used to host those tools is maintained to Claranet standards.
Additional Security controls features	• Participation in compliance audits – from time to time it may be required for Claranet engineers to participate in internal or external customer compliance audits in order to review policies, controls, and provide demonstrations. These should be raised as a Service Request with a minimum of three (3) weeks' notice. • Additional compliance reports or content that may be required. • Monthly reporting on security and data compliance controls.
Managed Endpoint Detection and Response	Upgrade to a Managed EDR service to benefit from 24/7 Security Operations Centre oversight from Claranet, to help protect workloads from confirmed threats and suspicious activity.
SSL / TLS certificates provided by Claranet	The Customer can purchase any combination of certificates from the following options: • **Basic**: Any website, intranet, or extranet conducting low volume or low monetary value online transactions. Includes £50,000 guarantee from certificate provider. • **Pro**: Any website, intranet, or extranet conducting medium to high-volume or medium to high monetary value online transactions. Includes £1,000,000 guarantee from certificate provider. • **Wildcard**: Any organisation that needs multiple certificates for a single domain name (e.g. web.domain.com,

	cdn.domain.com). Includes £1,000,000 guarantee from certificate provider. Renewals will be made for the duration of the contract unless the Customer instructs otherwise in writing through the change control process.

5. Managed Service

This Service is a managed service and this Service Description will be read in conjunction with the CXMS, which provides a framework for Claranet's core support experience and describes what the Customer can expect from any standard managed service solution provided by Claranet. This Service Description is intended to complement the CXMS and provide details specific to the Service. In the event that this Service Description conflicts with CXMS, the provisions of this Service Description will prevail to the extent of such conflict.

6. Roles and Responsibilities

The Customer, or any appointed third parties, acknowledge and agree to perform its responsibilities. Claranet's delivery, implementation and performance of the Service is dependent upon the timely and effective completion of the Customer's roles and responsibilities and/or as per Claranet's reasonable instructions. If the responsibilities as set out below are not met, and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

Responsibility	Description
Provide a suitable primary contact for the length of the Service.	To ensure smooth delivery of the Service, the Customer must provide Claranet with a primary contact with the relevant knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service Description and/or the SOW.
Access to support, key staff and stakeholders.	The Customer must provide key staff and stakeholders, both internal and external (where relevant), are available for engineer visits, meetings and/or workshops. The Customer will provide the necessary access to support

	and relevant personnel. However, the Customer will be responsible for ensuring all communications to all key or relevant Customer managed stakeholders regarding the Service for the duration, including any technical change and/or approval required.
Provide a safe and suitable working environment.	Where Claranet employees are required to attend Customer and/or third-party premises, the Customer must ensure that Claranet employees are provided with a safe and suitable working environment.
Provide information required by Claranet.	The Customer shall provide any information requested in the format specified by Claranet within five (5) working days, unless agreed otherwise in writing.
Responding to project requests by Claranet.	The Customer shall respond to any project-related request made by Claranet within five (5) working days. Unless agreed otherwise in writing.
Reasonable and timely cooperation	The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet.
Notifications regarding maintenance	The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance scanning, verifying, and identifying vulnerabilities within the Customer's Assets.
Changes to information	The Customer will ensure that technical details are kept up to date by submitting to Claranet to update the relevant details.
Patching	Where agents are required to patch the platform, e.g. virtual machines, Claranet will deploy those agents using the standard Change Management process.

	Where resources are in-scope for patching, Claranet will tag the resources with patching schedules in accordance with Claranet's tagging standards.
Monitoring	Claranet will need to liaise with the Customer where agents are required to monitor, e.g. virtual machines, appliances, containers. These agents will be deployed using the standard Change Management process. Claranet will ensure that in-scope resources will be tagged to Claranet's tagging standards for the purposes of monitoring.

6.1. Pre-Requisites

Before Claranet can commence the Services, the Customer is required to complete the following pre-requisite activities to ensure that the Services can be delivered successfully. If such pre-requisite activities are not met by the Customer, then this may have consequential adverse impact on the delivery of Services and may prevent Claranet from delivering on its obligation and/or require changes in a Change Request Form to remediate any impact.

Pre-requisite Activity
Claranet will undertake a health check to evaluate environment readiness. This may lead to a quoted remediation project if the current environment is not deemed ready to onboard.

Note: In the event a Pre-requisite Activity is not completed, the delivery of Service may be delayed, quality of Service may be impacted and/or additional costs may be incurred to deliver the Services. In addition, the Service shall not be subject to the SLAs or Service Credits (if applicable) and shall be provided on a reasonable endeavours basis until the above activities are completed.

7. Delays and Cancellation Terms

1. Professional Services must be used within 6 months from the date of Customer's signature of the Order Form and at expiry of this period, Claranet may invoice the full remaining Professional Services Fees and the Customer will pay those Fees in accordance with the Agreement. Thereafter, the Customer will have a further 6 months to use those remaining Professional Services, after which they will expire on such date if unused. Unless agreed otherwise, Professional Services are non-refundable.

2. The Customer agrees and acknowledges that Claranet will estimate the time required to complete the Services and that additional days of Professional Services may be required to complete the Services. Claranet shall notify the Customer where it determines in good faith additional days are required to complete the Services and such additional days may then be authorised by the Customer in accordance with Change Request Form or an additional Order Form.

3. If the Customer postpones a booking (e.g. a workshop, meeting or a call) at short notice, then the following will be charged by Claranet, depending on the amount of notice given:

Notice for Postponement	Postponement Fee
Less than 15 working days but greater than 10 working days	50% of the Fees associated to the booking
Less than 10 working days but greater than 5 working days	75% of the Fees associated to the booking
Less than 5 working days	100% of the Fees associated to the booking

4. If the Customer seeks to cancel a Service/s before the expiry of the Initial Term or Renewal Term, Claranet will automatically invoice and the Customer shall pay for cancellation charges equivalent to the total Fees that would otherwise have otherwise be payable for the remainder of the Initial Term or Renewal Term of the respective Service/s, unless agreed otherwise.

5. Once the cancellation has been processed by Claranet, the Customer shall follow Claranet's reasonable instructions to decommission any hardware and to cease access to relevant systems that the Customer received as part of the Service.

8. Assumptions and Exceptions

Service delivery may be affected if the following occur below. Where relevant and to the extent any Service Levels set out herein are impacted by the below, Service Credits will not apply as a result.

1. It is assumed that where required as part of the Service, access to the Customer's IT infrastructure is quickly established and retained for the duration of the Service. Any issues relating to access and permissions may result in work being halted or delayed until such access is resolved, or cause failures in delivery because Claranet personnel are unable to access the Customer's relevant sites.

2. Where software licences are not provided as part of the Service, it is the Customer's responsibility to ensure they have the appropriate subscriptions and licences as required to benefit from the Service. The costs of such licences and subscriptions are not included in the price of the Service as set out in this Service Description unless otherwise provided in the Agreement.

3. Claranet is not responsible for any failure of any component for which Claranet has no control over, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer.

4. Claranet excludes responsibility for meeting any Service Levels to the extent that meeting the Service Level is affected by the following exceptions hereunder and Service Credits will, therefore, not be paid if the outage occurs from such exceptions:

    a. if the Customer is in default under the Agreement;

    b. in the event that the Service is unavailable due to any component, event or situation not wholly within the control of Claranet, including but not limited to a failure of a component that Claranet is not responsible, electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;

    c. in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;

    d. in the event that the Service is disrupted or unavailable due to viruses, unauthorised users or hackers;

e. in the event that the Service is unavailable due to changes initiated by the Customer, whether implemented by the Customer or by Claranet on its behalf;

f. in the event that the Service is unavailable as a result of the Customer exceeding system capacity;

g. in the event that the Service is unavailable due to viruses, not arising from the failure or breach of Claranet or Claranet's Service;

h. in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;

i. in the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;

j. in the event that the Service is unavailable due to Customer's third-party contractors or vendors or anyone instructed by the Customer gaining access to Claranet's network, control panel or to the Customer's website at its request;

k. in the event that the Service is unavailable due to a force majeure event;

l. in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;

m. in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct or of others authorised by the Customer to use the Services provided by Claranet;

n. in the event that the Service is unavailable due to any failures that cannot be corrected because the Customer are inaccessible or because Claranet personnel are unable to access the Customer's relevant sites.

9. Terminology

Unless otherwise specified, capitalised terms used in this Service Description shall bear the same meanings as those used in the Master Service Agreement, unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

Terms	Definition
Application Programming Interface (API)	A structured set of methods to interact between systems with code.

Content Delivery Network (CDN)	A geographically broad set of servers close to users that can cache web content such as web pages, images, JavaScript and video for a faster, more performant experience without affecting the backend servers.
Continuous Improvement / Continuous Deployment (CI/CD)	A practice to automate and streamline building, testing and deploying code, increasing reliability and reducing the burden of repetitive tasks.
Central Processing Unit (CPU)	A core part of a computer, responsible for processing instructions written in code and producing outputs based upon those instructions.
Customer Experience for Managed Services (CXMS) Document	The CXMS document provides a framework for Claranet's core managed support experience and describes what a customer can expect from any standard Managed Service provided by Claranet. It outlines the responsibilities of both Claranet and the Customer, including how to log and escalate cases, how SLA targets are prioritised, set, and achieved, as well as the tools used to perform these functions.
Distributed Denial of Service (DDoS)	A form of attack on a computer network to prevent it from functioning either partly or fully, using a set of computers (that may have been compromised in a cyber attack) dispersed across the world.
Domain Name System (DNS)	A set of servers that provide lookups to IP addresses for a computer, translating a domain name from text into the correct IP for that computer.
Financial Operations (FinOps)	A cloud management practice that promotes shared responsibility for cloud computing costs and performance across different teams, like engineering, finance, and business.
Infrastructure as a Service (IaaS)	An abstraction of computing hardware that takes away responsibility from businesses of maintaining that hardware, to provide access to computing resources over the internet, typically on a pay as you go basis or contract basis. Allows for businesses to get temporary access to this hardware, providing scalability and flexibility.
Infrastructure as Code (IaC)	A practice of managing computing infrastructure using configuration files and code rather than manual interventions, allowing for automation, improved consistency, and version control.
Internet Protocol (IP) address	A set of characters (either numeric or alphanumeric) with separators, to identify a device on a network or the internet.

Operating System (OS)	A piece of software that manages computing hardware, memory and processes, and any software designed to run on that software.
Platform as a Service (PaaS)	A cloud computing model that provides developers with a platform to build, deploy, and manage applications without the complexity of managing the underlying infrastructure.
Remote Desktop Protocol (RDP)	A protocol used by Microsoft to connect remotely to and control another computer on a network.
Secure Shella (SSH)	A network protocol that provides a secure way for computers to communicate and exchange data over an unsecured network, commonly used to login remotely to a computer.
Secure Sockets Layer (SSL)	A method of connecting to another computer in a secure manner, using a certificate or set of certificates to verify the identity of an organisation. The more modern replacement for this method is TLS.
Transport Layer Security (TLS)	A method of connecting to another computer in a secure manner, using a certificate or set of certificates to verify the identity of an organisation.
Virtual Machine (VM)	A software based representation of a physical computer, allowing users to interact with it and run programs and an operating system on that representation like a physical computer.
Virtual Private Network (VPN)	A digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet.