Claranet Cyber Security Service Description

Managed Detection and Response for Microsoft Sentinel

v.1.1.3

Contents

1

1 Service overview

Claranet provides real-time analysis of security alerts that are generated by applications, network devices, hardware, and end points on your network, alerting you to any risks or breaches.

Cyber-attacks are common. Preventative measures are well understood and are widely adopted in an attempt to block the threat. However, the ability to disrupt an active attack is still out of reach for most organisations. Fast reactions to prevent a potential breach requires a combination of technology and resource. A dearth of expertise and the high cost of sustaining a quality service, means that many organisations are looking to managed security service providers to fill this gap.

The Claranet Managed Detection and Response service for Microsoft Sentinel (or "Microsoft MDR") provides fast reactions to threats and high-quality alerts enabling you to quickly protect your business and frustrate the attacker's progress. Analyst driven, we provide real-time investigation of security alerts generated by applications, devices, hardware, and end points on your network. You receive valuable information triaged and analysed by the Claranet Security Operations Centre (or "SOC"), on a 24x7x365 basis, enabling you to contain even the most complex threats to your organisation.

Adaptable to your business goals, the modular service can be delivered to suit everything from compliance drivers to budgetary constraints and augmenting existing capability to advanced threat hunting.

We've got you covered.

This Service Description describes the Service Claranet Cyber Security provides and details your ("the Customer") responsibilities in relation to this Service. This Service Description forms part of an Agreement between the Parties and is subject to the terms of the Claranet Master Services Agreement 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.

The Customer expressly agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. In the event Claranet completes additional services, activities and/or deliverables upon the written request or at the direction of the Customer, the Customer shall be responsible for the payment of all Fees and expenses associated therewith.

1.1 How the service works

Managed Detection and Response comprises four core components:

- Security Incident and Event Monitoring software (SIEM)
- Threat Intelligence feeds
- A team of expert security analysts (SOC Team)
- User and Entity Behaviour Analytics

There are many levels available (see below) which enables the Service to be tailored to your specific needs and the available levels of technical experience within your company.

1.2 The Managed Detection and Response cycle

There are a number of stages within the Microsoft Managed Detection and Response cycle which ensure that the Service is configured correctly and evolves in line with experience.

Identify: Identify all of the assets within your organisation and to create an understanding of the management of the cybersecurity risk to your systems, data, assets, and your overall capabilities.

Architect: Design the Service to meet your corporate and business goals.

Protect: To monitor all the security events for indicators of compromise.

Response: Build an investigative report that shows what the compromise was and exactly what we found.

Optimise: To continually evolve the system in line with any changes to both internal and external threats.

The quality and depth of your Service is defined by the storage, detection and response options that you choose to build your Service with.

1.3 Storage options

MDR for Microsoft Sentinel is a cloud-based, highly-available SIEM platform, that is external to your network, to house data for 90 days with different options to extend this beyond.

Data storage locations can also be requested based on geographic location, but by default a UK data centre will be selected. The solution uses the same network architecture regardless of customer. Using this framework allows for the ability to scale up or down as required to respond to your business needs.

1.4 Service features summary

Feature	Description
Claranet Online	The Claranet Online portal is your primary contact point for the Service. Whenever there is a new Incident ticket that requires your attention or access to the Monthly Reports, you will receive a notification from Claranet Online. This is the location where you will raise queries or respond to Incident tickets if required.
Incident Detection	Event information, received from log sources on your network, are sent to Sentinel. If the Events meet the criteria of a detection rule, an Incident ticket will be created which is then reviewed, analysed, and prioritised by our Security Analysts according to the Incident Response matrix.
Incident Notification	You will receive Incident Notifications for Priority 1 to Priority 4 Incidents in Claranet Online. While you do not receive a notification of Priority 5 Incidents directly, the totals are displayed in the monthly reports on Claranet Online. For more detail on the Notification levels, please see the " Service levels and service credits" section.
Incident Management	We will make recommendations on prevention techniques, root cause analysis (as far as the analysts can go with the log investigations), identifying the initial attack vector and provide you with remediation techniques. This includes attending calls with you and with members of your team to discuss the attack in more detail.
Threat Intelligence	Threat Intelligence uses open sources, which include publicly available information regarding Indicators of Compromise (IOCs) such as domains, IP addresses, file hashes etc., and closed sources such as UK Government, other customer deployments, and working closely with other security business units within the Claranet group. This information is fed into the Sentinel Instance and used by the SIEM to enrich Incident investigations. The Analysts will review the Incidents and follow the notification path based on the priorities outlined in "Service priorities and categories" section.

Response Actions	Delivering the Service involves the investigation of, and potential initiation of "response" actions on the Customer's live systems on its current infrastructure. This may therefore have an impact on current workloads and environments. Response Actions will be discussed with and authorised by the Customer during onboarding.
Threat Hunting	Threat hunting involves our Analysts performing proactive searches for potential breaches. These threat hunts search for IOCs based on Tactics, Techniques and Procedures (TTPs). Threat hunting for specific TTPs involves having a deep understanding of the MITRE ATT&CK® Matrix for Enterprise. Our Analysts will develop hypotheses around how a threat actor may have gotten into your environment and what they may be doing once inside. Hunting queries are then developed to manually search for evidence to support the hypotheses. Should anything be found within your environment, an Incident ticket will be raised.
Tuning	The purpose of tuning is to remove as many false positives as possible to ensure that Incident notifications remain relevant. Tuning will be performed continuously throughout the life of the service. Your feedback via an Incident ticket on whether or not an alert is legitimate expected activity is required to allow us to tune efficiently.
Monthly Report	A Monthly Report will provide a summary of the Incidents discovered during the month, all P1 to P5 Incidents, and outcomes of threat hunting.
Quarterly Review	Once per calendar quarter, the SOC Team will conduct a Quarterly Service Review with you. During this meeting we will discuss the Incidents processed, break downs of false positives / benign Events vs Incidents, SLA metrics that have been met, service improvement recommendations, etc.
User Behaviour Analytics	Using native identity connections Claranet will extend protection beyond simple events and actions to cover all users and their behaviour in the organisation. Working with the Customer Claranet will identify key users and systems and monitor for not only events taken by these users but also how the system interacts with them, allowing the SOC Team to identify outliers and suspicious behaviour before an incident is raised

Custom Detection Rules	The Customer will have the ability to request Custom Detection Rules that are specific to the Customer's environment. These can be requested via Claranet Online as part of the Change Management process.

.

2 Consult

We will work with you to establish the scope of your service and provide an indicative quotation.

2.1 Scene Setting call

We will start the process with a scene setting call, during which we will establish your high-level project drivers, goals, and requirements, and how the Service can assist in meeting these.

2.2 Scoping Form

You will then be provided with a Scoping Form which gathers information about the type and quantity of your log sources you would like to monitor. It is extremely important to complete the form accurately as errors can lead to underestimating or overestimating the Data Tier leading to insufficient storage (lost logs) or an increase in the cost. We will help you complete this form.

Once the Scoping Form is complete, we will provide you with an indicative quote for the Service.

Responsibility	Claranet	Customer
Scene Setting call: Meeting to gather initial information regarding your specific requirements.	✓	
Scoping Form: Provide details of the type and quantity of all log sources to be included in the scope.		✓
Indicative Quotation: Provide pricing including costs for the installation, configuration and tuning of the system; licence costs, and monthly managed service charges.	✓	

3 Design

If you agree to proceed, then we will start work on your solution design and finalise your quotation.

3.1 Solution workshop

Our Solution Architect will arrange a workshop with you to understand your technical requirements, the devices that are deemed to be in scope, including count and location, the number of Sensors to be deployed, data storage, Data Tier estimate, log sources and the relevant features to be enabled, design considerations as well as any other supporting information required to produce the final design.

3.2 Statement of Works

Once the contract is confirmed, the Statement of Works (SOW) will be finalised, using all the requirements gathered from you and, where applicable, any third parties, colleagues, or any other relevant source.

The SOW will also contain a clear Success Criteria defined for Service deployment.

3.3 Order Placed

Once agreement is in place regarding the scope of the service as documented in the SOW, pricing will be finalised, and the order can be placed.

Responsibility	Claranet	Customer
Solution Workshop: We will organise a workshop by conference call to validate and capture technical requirements for the SOW.	✓	
Statement of Works (SOW): The SOW will form part of the contract and will be updated upon any change requests during the contract period.	✓	
Final Quotation: We will provide a final quotation based on the SOW.	✓	
Project Manager: A Project Manager will be assigned to ensure to align resources and ensure you understand the tasks, deliverables and milestones.	✓	

4 Build

Onboarding of the Service typically takes 12 weeks but will be dependent upon the size and complexity of your estate and you completing the Technical Pre-Requisites within 4 weeks.

4.1 Delivery Kick off call

Onboarding starts with a kick-off meeting where our engineers will discuss with you, in detail, the log sources that are in scope to be monitored by the Service. You will then use this information to complete an Asset Verification Form detailing the log sources to be onboarded.

4.2 Asset Verification Form

All log sources to be monitored will be documented in the Asset Verification Form, which will be tracked against the SOW to ensure that there will be no discrepancies. If we identify a change in scope, it will be managed by the Change Request process.

4.3Technical Pre-Requisites

We will use the Asset Verification Form to create a set of Technical Pre-requisite instructions that you can use to configure your log sources.

You will be required to configure your log sources and network topology in accordance with the Technical Pre-Requisites instructions. This will allow the logs to be forwarded to the collectors, connectors, or Sentinel.

Responsibility	Claranet	Customer
Delivery kick off call: We will set up a kick-off meeting with you.	✓	
Asset Verification Form: You will complete the Asset Verification Form.		✓
Technical Pre-requisite instructions: We will create the Technical Pre-Requisite instructions.	✓	
Technical Pre-requisites: Prior to onboarding any log sources, you must complete the Technical Pre-Requisites.		✓

4.4 Onboarding log sources and service features

Once the technical pre-requisites are in place, our engineers will assist you with onboarding one of each type of in scope log source - a process that will normally take 30 days. As the log sources are onboarded, tuning will begin.

After 30 days, regardless of whether onboarding is incomplete due to Customer’s delay on preparing log sources for onboarding, the Service and billing will commence.

Thereon, we will continue to work with you to onboard and tune any remaining in scope log sources and features as documented on the SOW and Asset Verification Form.

Responsibility	Claranet	You
Tuning: Remove the false positives being generated on the system to establish a baseline of the network and increase accuracy in detection. Tuning will be an ongoing part of the Service, and additional tuning of Events may occur during remediation and notification.	✓	
Tuning sign off: All tuning and filtering actions will be raised within an Incident ticket for approval. Where no response is received, agreement will be assumed.		✓
Features and functionality: We will ensure the availability of the solution’s features and functionality of the detection element, such as, Asset Detection, Event Correlation and Reporting. The configuration options will be removed from your view and the SOC Team will retain all configuration rights and views. Administration accounts will not be provided, unless under special agreement and the business justification identified.	✓	

4.5 Infrastructure setup and changes responsibilities

Once the technical pre-requisites are in place, our engineers will assist you with onboarding one of each type of in scope log source - a process that will normally take 30 days. As the log sources are onboarded, tuning will begin.

After 30 days, regardless of whether onboarding is incomplete due to Customer’s delay on preparing log sources for onboarding, the Service and billing will commence.

Thereon, we will continue to work with you to onboard and tune any remaining in scope log sources and features as documented on the SOW and Asset Verification Form.

Responsibility	Claranet	You

Security Operations Centre: We will deploy the sentinel instance and manage the build and communication between the SIEM and the service management platforms.	✓	
Infrastructure changes: You will be responsible for making changes to your infrastructure to ensure the solution is working correctly. This may involve making changes to the firewall configuration to allow ports for communication with log sources and update servers etc.		✓
Group policy changes: You will be responsible for making changes as required to your group policy, network settings, logging settings and levels, to ensure that the solution is working as proposed and that it is collecting the relevant information.		✓
Service accounts: You will be responsible for creating service accounts as required and ensuring that We can access resources under the service account. Multiple accounts may be required depending on the user access management system and the ease of auditing.		✓
Ports and IP addresses: It will be your responsibility to allocate external IP addresses as required to allow for remote management of the server(s) and software. (Example: Hardware deployments). Allocate internal IP addresses for the software and hardware that is used to collect logs and to provide network addresses for the operation of day-to-day activities.		✓
Emails and escalations: You will have to define an escalation process, if required, with points of contact that can be contacted in an emergency. In addition, you will have to configure the necessary email addresses and accounts to be used for notification purposes.		✓
Internet connection: You will have to provide a connection out to the internet that is routable from the server deployed zones.		✓
Ownership: Upon the expiration of the contract, we will retrieve any hardware assets and may need to access cloud systems to remove Sensors and proprietary rule base. Claranet access to the workspace will be revoked, but any unique configuration and data will remain in the client's Azure tenancy including the Customers Sentinel instance.		

5 Manage

Once configured and in place, the Managed Detection and Response Service will continue to monitor your infrastructure within the agreed scope and notify you of any security events that have been detected. The managed Service comprises many areas that are brought together once the Sensors have been deployed and are passing data to your central data store. These areas have professional analysts to support any automated functionality and provide an enhanced Service.

5.1 Service deliverables

The Managed Detection and Response Service will deliver the following, based on a standard deployment:

- Customer maintenance
- Change management
- Adding additional log sources

Customer Maintenance

If you have a Service outage (planned or otherwise) with regards to the Sensors deployed, your will be responsible to notify the SOC Team. If no notification is given and the Sensors are taken down for any reason, then the outage will be treated as an Incident. If the Sensor is offline for a period, there is a high probability that Events will be lost during the time the Sensor is offline.

Responsibility	Claranet	You
Customer Maintenance: You will be required to notify us if there will be any outage that will impact the Sensors deployed on your network.		✓

Change Management

We shall request written approval from you before a change can proceed to be implemented and if any specific time for implementation is required. Below is a list of Change types:

Change type	Definition	Example Changes
Simple Change Request (SC)	A simple change is one that carries a low impact on the Service or business operation.	• Change or removal of key contact(s). • Rule suppression for example you determine that a P1-4 ticket is standard business practice. • Request for information

Complex Change Request (CC)	A complex change is one that carries a moderate to high impact to the Service or business operation. Where Claranet deems a change to be complex (warranting specialist engineering or excessive time and resources to plan and execute), then Claranet may advise on a charge for these requests. Claranet will assist in making clear as to whether or not a given request is determined to be chargeable.	• Custom rule request. • Additional log sources to be monitored. • Extraction of log history. • Assistance with the removal of elements of the systems from your environment.
Complex-Contract-Affecting Change Request (CCA)	A complex-contract-affecting (CCA) change is where the request alters the Service in such a way as to no longer operate in the manner set out under the original Statement of Works. CCA’s may have an impact on the ongoing billing or commercial agreement of the Service. Claranet will assist in making clear as to whether or not a given request is determined to be complex-contract-affecting. Once a change request is implemented the SOW will be updated and authorised by both parties before being implemented.	• Additional log sources to be monitored that pushes the Data Tier over the contracted limit as stated in the SOW.

Adding additional log sources

Through the change process, you will be able to add log sources to the Service during the contract period by making a request through the Claranet Online portal.

Before we can start monitoring all your Events on a newly requested log source, there are certain configurations that must be in place to ensure that the data store is receiving all of the relevant Event logs.

Any additional log sources you wish to add will be evaluated, configured, and set up correctly.

If you do not notify the SOC Team, any additional log sources will not be monitored and will be considered out of scope. All additions will be recorded on your Asset Verification Form.

Appendix A

A.1 Optimising your Service

Within the Build process, there are many areas that can be tuned to suit your individual requirements and the specifics of your network. Details of these tasks can be seen below:

Responsibility	Claranet	You
Log source preparation: Make the relevant changes to the network devices and or configurations to ensure that the log source onboard can be met. Any disruption to the onboarding will lead to exceptions being formed to hinder the success criteria of the deployment. The product feature may require updates or upgrades to software packages. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓
Log source onboarding: Confirm that the log sources in scope have been added to the system and are sending logs to the Sensor and Sentinel. Confirm that the log source data is being parsed correctly and the relevant plugins areenabled. Once all assets deemed in scope are onboarded this will meet one part of the success criteria. Claranet will guide the onboarding of the log sources by grouping devices and ensuring a smooth onboarding via a phasedapproach.	✓	

Responsibility	Claranet	You
Windows agent requirements: Ensure that the agent dependencies are met: • 64-bit operating system • PowerShell version 3 at a minimum. Windows OS 10+ • Windows Server 2016+ Admin credentials for the host are provided. Failure to provide this may result in the product feature not being made available and/or a reduction in Service or exceptions to the success criteria being met. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓

Linux agent requirements: Ensure that the agent dependencies are met: • 64-bit operating system • Kernel 5.0+ • Supported Distribution Admin credentials for the host are provided. Failure to provide this may result in the product feature not being made available and/or a reduction in Service or exceptions to the success criteria being met. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓

Responsibility	Claranet	You
Threat Intelligence configuration: Configure the relevant threat intelligence account depending on whether standard or analyst driven option is selected, ensure the data is downloaded and presented in the system ready for use with correlation. A non-exhaustive list of these sources is : OTX, NCSC CiSP, RiskIQ. Claranet review and swap threat feeds throughout the life of the service to ensure a broad range of sources and expertise	✓	

Responsibility	Claranet	You
Integration configuration: Configure the integration from Sentinel to the ServiceNow platform and ensure data is reaching the service management platform. If you have access to the system, you will receive a read only account. However, if any configuration changes are made that impact the data integration between the SIEM and ServiceNow as a result of changes made then this downtime or loss of data is not the responsibility of Claranet.	✓	
Tuning sign off: Sign off of all tuning and filtering actions completed on the system and agree with the baseline that has been set.		✓
Tuning: Tune the system and remove the false positives being generated on the system, this is done to accept a baseline of the network and increase accuracy in detection. Tuning is an ongoing part of the Service and driven by the false positive rate we detect. Any tuning rules will be raised as a ticket and worked with the customer to ensure no rules are put in place that will create blackspots in the detection or otherwise filter out a critical event. .	✓	

A.2 Security Incident Process Flow, Service Levels Agreements and Service Credits

Response times shall be based on the level of severity of any issue that may occur; they are as follows:

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Definition	Critical severity, issue has a critical impact on the customer and their environment and may have a severe impact on availability, performance or functionality of live service. Requires immediate action from the customer (or action has already been taken by the SOC).	High severity, issue has a high impact on the customer and their environment but currently no or limited live service degradation. Requires immediate action from the customer (or action has already been taken by the SOC).	Medium severity, issue may moderately impact the customer or their environment and requires action from the customer (or action has already been taken by the SOC).	Low Severity, information ticket. No action required from the customer, but it should be brought to their attention.	No severity. No action required from the customer and no need for it to be brought to their attention (non-security issue, BAU, benign, false positive etc.)
Triage *	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.
Response time	Notification within 15 minutes from the point of classification.	Notification within 30 minutes from the point of classification.	Notification within 2 hours from the point of classification.	Notification within 4 hours from the point of classification.	Not applicable.
Notification process	Notification via Claranet Online with a follow up telephone call.	Notification via Claranet Online with a follow up telephone call.	Notification via Claranet Online.	Notification via Claranet Online.	Not applicable.
Ticket Closure	P1 incident tickets will never be set to auto resolve.	P2 incident tickets will never be set to auto resolve.	P3 incident tickets will be set to resolved after 5 days. The tickets will remain open in Claranet Online where they can be responded to by the customer. After a further 3 days with no response, the ticket will close.	P4 incident tickets will be set to resolved after 3 days. The tickets will remain open in Claranet Online where they can be responded to by the customer. After a further 3 days with no response, the ticket will close.	P5 incident tickets closed by the SOC Team.
Triage SLA Service credit	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee
Response SLA Service credit	5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	N/A	N/A	N/A

* In instances where duplicate tickets are created for an incident. The triage time for the first ticket relating to that incident will be used.

Contacting the Security Operations Centre

Purpose	Who to contact	Contact Info
Support Primary	SOC Team	https://online.uk.clara.net (Primary)
Support Secondary	SOC Team	Phone: 0330 390 0500 (Secondary)
Platform Support	SOC Team	https://online.uk.clara.net (Primary)

Operational Hours

Category	Hours
Security Operations Center	24x7 (12 Hour Shift Patten)
Security Engineering	Monday – Friday 09:00 – 17:30
Account Management	Monday – Friday 09:00 – 17:30

Contacting you

Authorised Security Contacts

An authorised security contact is defined as a decision-maker on operational issues pertaining to the Claranet Managed Detection and Response Service. Contact information must be complete in Claranet Online to ensure we contact the correct person.

Designated Services contacts

A designated Services contact is defined as a decision-maker on a subset of operational issues pertaining to the Claranet Managed Detection and Response Service. Claranet will only interface and provide updates to a designated point of contact regarding security incidents dependant on your nomination of the individual or group.

Portal users

The portal users will receive the same access to the portal, setting up individual accounts for the users and notifying them of when an incident is confirmed. Claranet will notify all members of your organisation that have been nominated within the 5-user limit. Should you require more user accounts please contact us to discuss your requirements.

Outages

The Managed Detection and Response Team will be responsible for the Service, if there is any issueimpacting patching or development work scheduled, you will be notified through the portal.

If there is a Service outage (planned or otherwise) with regards to the Sensors deployed, your responsibility is to notify the Managed Detection and Response Team. If no notification is given and the Sensors are taken down for patching and maintenance of your VMWare or Hyper-V infrastructure, then the outage will be treated as a P1 incident, and a telephone call will be made to whoever the on-call or in hours contact is. If the Sensor is offline fora period of time, there is a high probability that events will be lost during the time the Sensor is offline. Details of outages to the Service will be detailed in the Monthly Service Report.

Common terms used

Terms	Definition
Managed Detection and Response (MDR)	Managed Detection and Response (MDR) solution providing 24/7 Incident detection, notification, and management.
Security, Information and Event Management (SIEM)	Platform that enables security personnel to detect threats, respond to security Incidents. For this Service Claranet uses USM Anywhere to collect log data so Claranet Security Analysts can investigate Incidents and block malicious activities.
CREST accreditation	The CREST accreditation means our policies, processes and competencies have passed the rigorous accreditation process. All members must complete an application process which examines its quality processes and procedures; compliance with standards compliance (e.g., ISO27001, ISO9001); professional indemnity insurance; contract management; informational security processes; complaint handing and conflict of interest policies.
Indicator of Compromise (IOC)	An Indicator of Compromise (IOC) is evidence of potential intrusion on a host system or network.
Tactics, Techniques and Procedures (TTP)	Tactics, Techniques and Procedures (TTP) describe the behaviours of threat actors. Tactics are the high-level description of the behaviour, techniques explain the general method used to achieve the goal, and procedures offer the steps used to carry out the attack.
Asset Verification Form	The Asset Verification Form details the log sources that are to be monitored by the Service. This is a living document and will be updated as new log sources are onboarded through the change management process.
Event	An action or occurrence that has been recognised and recorded by a log source such as operating system, server, firewall etc. These Events are fed in to the SIEM where Detection Rules and the SOC Team will determine if they are an Incident.
Incident	An Event that has been determined that it may indicate a compromise to the customers security and requires further investigation.
Detection Rules	These are the rules that the SIEM will run on the Events that are fed in to it to determine if they require further investigation by the SOC Team.
Data Tier	This is the amount of Event log data that is fed in to the SIEM by the customers log sources.

Managed Service	The MDR service that the SOC team deliver to the customer through incident triage and response and the Engineering team deliver through platform support.
Sensor	A log collection utility that may be internal or external to the Customers network.

Service Levels

If Claranet fails to deliver the stated Service level, Claranet agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

Service level availability guarantee

Service levels are set out in the table entitled “Service levels showing priorities and timescales”.

A.2.1 Service level credits

In the event that you and Claranet agree that a Service Credit is due in a given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected Service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a customer can receive in each calendar month relating to this agreement is fixed to 25% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in the Agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Compensation claims

Compensation claims must be submitted within 30 days from the point the Customer is made aware of the breach. All claims must be submitted to the appointed Account Manager in writing by email. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating Service levels..

Exceptions

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

- if you are in default under the Agreement;
- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
- in the event that the Service is disrupted due to unauthorised users or hackers;
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or by Claranet on your behalf;
- in the event that the Service is unavailable as a result of you exceeding system capacity;
- in the event that the Service is unavailable due to viruses;

- in the event that the Service is unavailable due to your failure to adhere to Claranet's implementation, support processes and procedures;
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel or to your website at your request;
- in the event that the Service is unavailable due to a force majeure event;
- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- in the event that the Service is unavailable due to your negligence or wilful misconduct of you, orothers authorised by you to use the Services provided by Claranet;
- in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by you;
- in the event that the Service is unavailable due to any failure of local access to facilities provided by you; and
- in the event that the Service is unavailable due to any failures that cannot be corrected because you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing technical contact details.

A.3 Cancellation of the Service

Responsibility	Claranet	You
Notice of cancellation: Give 90 days' cancellation notice for the Service to Claranet prior to the end of the contract term in writing to the MSP Cancellations team. Any support you need including extraction of logs/history or assistance with the removal of elements of the system from your environments will be charged as time and materials at the current Claranet consulting rate at the time of carrying out the works.		✓