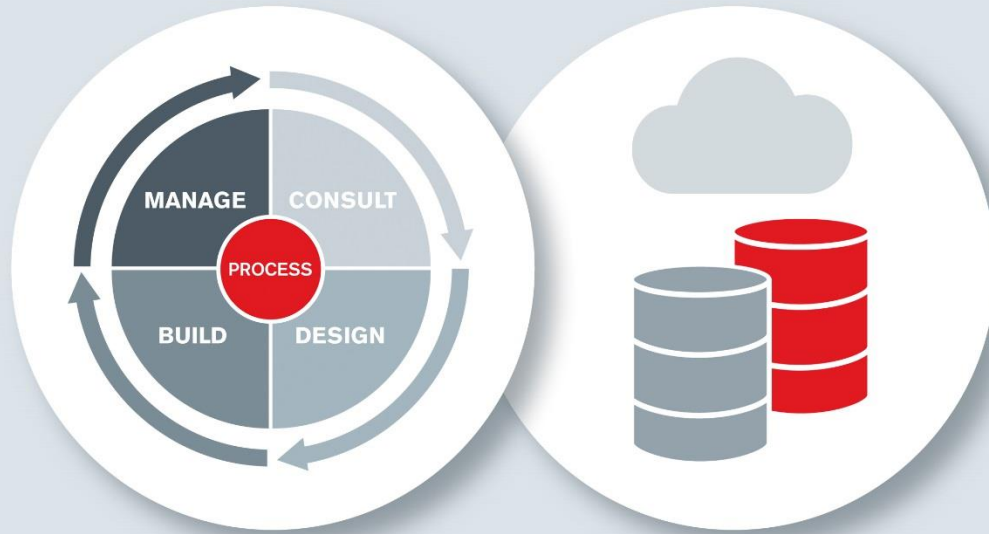


Claranet Service Description



Enterprise Backup

Enterprise Backup is a remote data backup service enabling you to back up and archive your data from any environment to a secure platform hosted in two mirrored UK-based Claranet Data Centres.

Version 10.1

Contents

Service overview	2
Consult	4
Backup and Recovery sales specialist.....	4
Design	5
Backup Assessment.....	5
Build	6
Setup and configuration.....	6
Project Management	8
Manage	9
In-Life Management	9
Network Operations Centre (NOC) portal	9
Help and support.....	11
Service Levels.....	11
Appendices.....	12
Claranet UK Data centres.....	12
Appendix: Components.....	13
The Enterprise Backup software.....	13
Appendix: Elements.....	14
Security.....	14
Pricing.....	14
Appendix: Support	15
Help and Support	15
Service Levels.....	16

The Service Description

This Service Description describes the service Claranet provides and details your responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Service overview

Enterprise Backup, powered by Asigra, is a remote backup and archiving service, enabling you to protect your critical data. The service utilises the industry-leading Asigra software which, once installed on your system, will compress, encrypt and transfer a copy of your selected data to a secure backup platform maintained by Claranet. This is mirrored across 2 Claranet UK data centres. Your backed up data remains encrypted at all times, protected by an encryption key defined by you. Claranet has no access to your data.

The service is based on agent-less architecture and does not require the software to be installed on every target server on your network: keeping deployment, management and maintenance time to a minimum.

The Claranet Enterprise Backup service will automatically back up new devices added to your network. The service is designed for complex systems and will support a multitude of environments - physical and virtual servers, various Operating Systems, databases and Public Cloud services. An easy to use interface allows you to make changes to your backup configuration and to recover data.

The service provides the facility to create multiple backup sets, each one allowing a different backup schedule and retention policy to be applied. You therefore have complete control over the overall number of versions, and over which, from all those that you have backed up, you wish to keep.

In addition, you have the option of utilising two storage tiers in our data centres; one for the data that you need to retain fast access to; and a second tier which provides a more cost effective archiving option for data you want to store long term.

The service covers installation, maintenance and the recovery of your data. Please note that while Claranet will provide step-by-step assistance and support in installing and configuring the service, you retain access to manage and make changes yourself, should you need to.

Installation and Configuration

Claranet can assist you in getting started with the service and provide guidance to help you to install and configure the software onto your network. The main component is the Asigra DS-Client, which can be installed on a server (or servers) within your environment. A Claranet engineer will be on hand to provide assistance during the installation. Further details can be found in the **Appendix**.

As part of your initial backup, you will be prompted to select the data that you wish to protect and the number of versions you want to keep for each backup set. The service can be configured to your needs: with a flexible retention policy, as well as the ability to adjust the frequency and timings of backups and even the compression method. Further details can be found in the Appendix.

Backing up

At the scheduled time, your Enterprise Backup service will compare the specific files you have selected within a particular backup set to establish whether changes have been made to the files since the last backup. If changes have been made, the changed section within the file is copied, compressed, encrypted at source, and sent securely across the internet to Claranet's Enterprise Backup platform in Claranet's data centre in Chelmsford, Essex. The Enterprise Backup service also checks that these changes can be successfully applied to the previous version to ensure that the file can be successfully restored. Your data is then mirrored every two hours to a second Claranet data centre in Hoddesdon, Hertfordshire.

Archiving

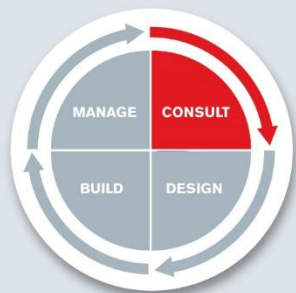
The service offers a secondary storage option for archiving data. This is referred to as Backup Lifecycle Management (BLM). BLM is set up and configured using the same Asigra DS-Client. It is recommended for use on files which you are less likely to restore and will not be changing. BLM cannot be used as a standalone service, but can be utilised in conjunction with the primary backup platform.

Recovery

You are able to initiate restoration of your files from the DS-Client without recourse to Claranet. A secure copy of your file(s) is retrieved from the data centre and made accessible via the DS-Client for you to download on to a suitable environment. You can choose to restore individual files in the event of accidental deletion or corruption, or all your files in the event of a total data loss.

The Network Operations Centre (NOC) portal

As part of the service, you will have access to a web portal, where you can view reports on different backup sets, download Asigra software components, related documentation, and user guides. The NOC portal will also allow for partial management of your DS-Client installation.



Consult

Claranet's consulting process ensures that you have the right information, the right recommendations, and the right service options available to you to achieve your business outcomes.

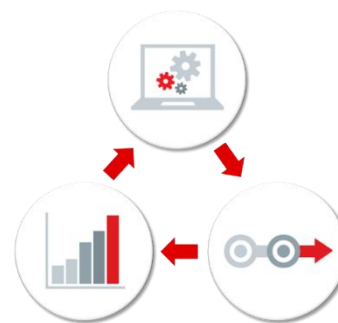
Understanding your business is paramount to ensuring that you have the right solution for your business outcomes. In the Consult stage, Claranet will discuss your business requirements with you prior to recommending a solution. Depending on the complexity of your requirements, one or more workshops between you and Claranet may be arranged in order to outline them in more detail. It may be the case that the implementation of your Enterprise Backup service is part of a larger project.

Backup and Recovery sales specialist

Claranet provides a Backup and Recovery sales specialist who has detailed knowledge within this particular field, or within your own specialist vertical industry, and will support your Account Manager and Solutions Architect with your proposal. Part of their role is to help ensure that the proposed technical solution will fit your business and achieve the outcomes you are looking for.

Claranet also has a number of pre-packaged assessments and audits that help to outline your readiness in respect to particular IT options.

The completion of these assessments follow a general pattern:



Current State

Performing a real life assessment of your current environment and understanding where your business needs, and your current technical setup, may diverge.

Future State

A vision of the future for your company, taking into account strengths, weaknesses, opportunities and threats.

Transformation

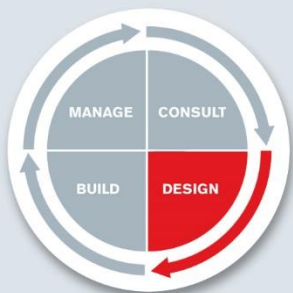
The enablement program to be undertaken as a priority to advance your organisation to the desired level of maturity.



What Claranet will do

Beyond service scope: When opportunities arise where Claranet can go beyond the bounds of the standard Enterprise Backup Service, one-off Professional Services may be beneficial. Details of this may be found in the Design section. Examples include:

- Invocation of a Disaster Recovery plan
- Full data recovery testing



Design

Your Claranet Enterprise Backup solution will be designed to meet your requirements. The decision as to how this fits within any business continuity solution is made in the Design stage.

Your solution may also require the use of a Solution Architect and if so, the output of this process may be a proposal document and a Statement of Works (SoW). It may be part of a larger document if the Enterprise Backup service is part of a larger solution. This forms part of your agreement and will provide the technical specifications for your solution.

Typically the technical design, if required, will be completed prior to order, but further detail can be refined once the order has been placed. Any technical design work is conducted on a 'reasonable commercial endeavours' basis and will be based on assumptions made by you and Claranet.



What Claranet will do

Deliverable: A proposal document and a Statement of Works which may be part of a larger solution document, and which forms part of your agreement which is detailed enough to allow a full quotation.

Standard level of design work: Produce design work on your proposed solution at a level commensurate with that of the market. It will be sufficient to allow further decisions to be made and may include input from a Claranet Sales Specialist.

Additional components: In the event that additional components are required outside of the SoW, Claranet will levy additional charges for the implementation and management of the modified solution. If this is the case, a new proposal and SoW document is produced. This must then be signed by you to acknowledge and accept the changes before any work is performed.



What you will do

Outline: Outline the purpose of any requirements to Claranet, in order to ensure that Claranet may assess whether the solution is suitable for the requirement.

Backup Assessment

Claranet can help you to tailor your Enterprise Backup service to your needs. A backup specialist can liaise with you to analyse your data and data change patterns, and, using relevant tools, suggest the best possible configuration. As part of this engagement, the Claranet specialist will assist you in installing the Asigra LAN Discovery tool on your environment, which will search for data on your network and provide useful insights and reports on file types and volumes, duplicates, changed and unchanged files, as well as growth patterns over a short period of time.

If you are unsure of the volume of data you need to back up on the Claranet Enterprise Backup platform, our specialist can assist you in designing your backup configuration based on these reports. As you are charged for the amount of data you store on the platform, this service ensures you only store exactly what you need to and helps to keep your costs to a minimum.

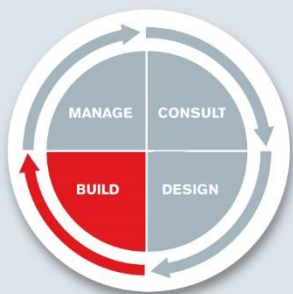


What Claranet will do

Specialist design: Produce technical design of your proposed solution based on your requirements. This may be completed by Claranet Specialist in that particular field. And charged on a Professional Services day rate basis.

LAN Storage Discovery: Asses your data environment, so that you can decide what to back up and what is less critical. Statistical backups can also provide assistance in estimating the required backup size and the change trends of your data.

Outcomes: Provide a full and detailed report on your available options and recommendations of the next steps to take.



Build

Claranet will assist with the installation and configuration of the service to ensure a copy of your data is stored in the Claranet data centres.

The Build section covers the steps involving the configuration and installation of the Enterprise Backup service according to the agreed specifications. Once set up, any future changes are explained as part of In-Life Management, details of which can be found in the Manage section.

Setup and configuration

Pre-installation

What Claranet will do

Schedule a call: Once your order is received by Claranet, a representative will give you a call and let you know what the next steps are. Shortly afterwards an engineer will be in contact to schedule a call to go through the installation.

Account creation and confirmation email: Create an individual account on the backup platform for you and provide an email with an attachment (CRI file) containing the account information and instructions on how to download and install the DS-Client software.

Provide Assistance during installation and configuration: Provide any necessary step-by-step assistance to guide you through the installation and the configuration of the Enterprise Backup software.

What you will do

Provide your details: Provide the correct details for your account to be set up on the main storage platform.

Confirmation Email: Follow the instructions in the email and keep the attachment provided (CRI files), to be used as part of the installation of the Enterprise Backup client.

What you will do

Minimum spec server for the installation: Make available a virtual or physical machine built to the minimum specifications as outlined in the Appendix for the DS-Client installation.

Download and installation: Download the Enterprise Backup client (DS-Client). During the installation, you will be asked for the CRI file that was attached on the confirmation email. This will automatically configure your local installation with your Enterprise Backup information retained on the main storage platform.

Internet connection: Ensure that each DS-Client has access to the internet and the required firewall ports are open in order to successfully complete backups.

Corruption: Ensure that all files to be backed up are not corrupted.

Initial configuration

What you will do

Encryption Key: Set a private encryption key and an account encryption key. Please note that you are responsible for maintaining your unique encryption key in a safe place and you retain control over who has access to this encryption key. It may be needed in order to restore your files and it may **NOT** be possible to restore files without it. Claranet will **NOT** maintain a record of your encryption key nor have access to your data.

Selection of the encryption method: During the initial setup, you will be asked to select the method of encryption for your files, ranging from DES 56-bit to AES 256-bit. The setting of AES 256-bit is used as standard.

Compression method: A standard compression rate is used but it is possible to select between two compression methods, LZOP and ZLIB, in order to balance between the time taken in processing and the residual file size.

What you will do

Data selection after the installation: After the installation is complete, select the files and folders from your Windows or Linux network that you wish to add to your backup set.

Scheduled backups: Schedule the time and frequency for the backup of each individual backup set. The Enterprise Backup service can maintain a number of backup sets running concurrently.

Continuous Data Protection (CDP): Choose this option as opposed to scheduled backups. This provides close to real time, end to end data protection. As a new file is added or an existing file changed, a new copy of the file is sent securely to your account on the Enterprise Backup platforms at Claranet's data centres.

Generations: Select the preferred number of generations retained on the Claranet Enterprise Backup platform for your individual backup sets. The default setting is 30.

Retention rules: Decide which of the generations that have been created are to be kept, it does not have to be the latest versions. (e.g. you may choose to keep 30 generations in total, and, although the files may back up once a day, this could mean that you choose to keep once a day for a week, once a week for a month, once a month for a year and once a year for 9 years!).

Archiving: If archiving is required, you set the retention rules for that backup set to copy the data from the main platform to the Backup Lifecycle Management storage platform and then delete it from the main platform. Consequently it is not possible to run an incremental backup method with the files in this backup set. This provides a more cost effective long term storage area for files that will not be changing further.

What Claranet will do

Account activation: Set your account to live mode, after you have successfully installed the DS-Client software.

Multiple DS-Clients

It is possible to set up more than one DS-Client on your network. This provides effective load-balancing and an increase in resilience. A single interface allows you to monitor all of your DS-Clients together.

File selection

Data Types and Environments Supported

By drilling down through your folders and sub-folders you can select individual machines (presented as members of your network). The service can protect different elements of your machines, depending on the DS-Client version (Windows or Linux), including:

- Files
- Folders
- Microsoft Exchange
- Microsoft SQL
- Microsoft Outlook
- Microsoft SharePoint
- Oracle databases
- DB2
- PostgreSQL
- Sybase
- Lotus Notes
- Lotus Domino
- MySQL
- GroupWise
- SAP
- IBM System i / Power 6,7

Any file selections can be easily changed using the DS-Client. For a full list of applications, please see the relevant documentation, available in the NOC portal.

Hypervisors supported: Enterprise Backup will interrogate and back up from the following hypervisors:

- VMware Virtual Machines
- HyperV Virtual Machines
- XenServer Virtual Machines

Data Types and Environments Supported

Cloud Services supported: Enterprise Backup can also back up your data from SaaS services such as

- Google Apps (Contacts, Calendars, Drive, E-Mail, Sites)
- Salesforce.com (Objects and schema)

Acceptance procedure

Once the backup solution is set up, the ongoing management falls under the In-Life Management process.

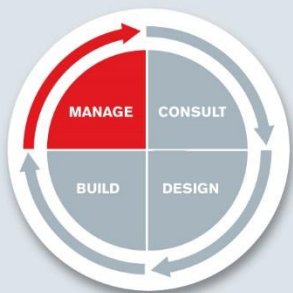
Project Management

Some Claranet projects are small, simple and very straightforward and the management of these is part of the normal operation carried out by your Project Co-ordinator who is already built into the cost of delivering your standard service. Other Claranet projects are much more complex and require more comprehensive project management to bring together the many elements that are needed. Claranet is conscious of the fact that the introduction of a Claranet Project Manager is a chargeable event but will suggest this when we believe it is justifiable and necessary. In addition, it may be that only a short time needs to be spent by a Claranet Project Manager in overseeing and authorising the Claranet project e.g. at the start of the project, where the project is then managed by a Project Co-ordinator, helping to keep your costs to a minimum.



What Claranet will do

Project Management: Allocate a Claranet Project Manager who is PRINCE2 qualified who will ensure that the project is initiated, implemented, carried out and closed according to PRINCE2 methodology and will be responsible for the overall control and management of the Claranet project. Full details of this can be found in the Project Management Service Description and from your Account Manager.



Manage

Your solution is managed In-Life by our Service Operations team who provide a pro-active, ITIL aligned service.

In-Life Management

Backups

With the initial backup, a full copy of the selected files is taken and encrypted whilst they remain on your machine. These files are then sent securely across the network to Claranet's Enterprise Backup platform in our data centre in Chelmsford, Essex. Every 2 hours, the data is replicated to a secondary data centre in Hoddesdon, Hertfordshire. The initial backup takes longer than subsequent backups. Subsequent backups are incremental and copy only those parts of files which have changed, along with a copy of any new files which have been added since the last backup.

Snapshot backup

If the initial backup is of an appropriate size, you can send your backup on a drive directly to the data centre. Please see your Account Manager for details on this option. The smaller incremental backups are stored separate to the original, allowing you to restore earlier versions of your files.

Data recovery and restoring files

You can restore either an individual file or a selection of files using the Enterprise Backup software. A secure copy of your file(s) is retrieved from the data centre and is restored directly to the server it is installed on.

What you will do

Selection: You will be responsible for adding and removing files and folders to and from your backup sets.

Successful Backup and recovery: You will be responsible for ensuring that the backups run as configured and that you can access and restore your data. During the creation of your backup sets, you configure the service to receive email or SNMP alerts to ensure that backups are completed successfully.

Network Operations Centre (NOC) portal

The Network Operations Centre (NOC) is a web-based portal where you access information on the configuration of your service, including reports from backups, the selected data backup sets, and BLM-archived data. Documentation and useful tools are also available for downloading. The NOC portal allows for the creation of restorable images from your BLM archive packages. Enterprise Backup logs are available to help with any troubleshooting of backup issues.



What Claranet will do

Network Operations Centre: Provide access to the Network Operations Centre (NOC) and send you log-in details and instructions when setting up your account.



What you will do

Browser compatibility: Ensure that a suitable browser is installed in order to access the NOC web portal. The NOC web portal is supported on the following browsers.

- Internet Explorer 8 or later
 - Mozilla Firefox 3.6 or later
 - Safari 4 or later
 - Google Chrome 10 or later
-

Planned changes, emergency maintenance



What Claranet will do

Notice: Provide at least seven working days' notice of any planned maintenance work where an outage is expected, wherever possible.

Supplier planned Engineering: Notify you of any supplier planned engineering works where it is likely that you will experience an outage within one day of receipt of the notification from our supplier wherever possible.

Notification: Notify your nominated contacts through two primary channels, Claranet Online and by email notification. An email is sent to the nominated contact and details are announced through the notifications in Claranet Online. The notification will contain the date and time of the maintenance, the reason, the service affected and the likely impact to you.

Problems occurring during planned maintenance: The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the planned maintenance window.

Emergency maintenance: Provide as much notice as possible and we will seek to ensure minimal disruption. Wherever possible, changes will be made at periods of low service utilisation. It may be necessary to make changes **without** prior notification to ensure the continued operation of the managed service.



What Claranet will do

Patching: Apply all critical patch updates on an as required basis.

Emergency outages: In some extreme cases, Claranet may require an emergency outage to rectify a problem. In such cases, Claranet will work with you to agree a mutually convenient time, but you agree that in such cases the problem cannot be rectified until the outage has taken place.



What you will do

Contact list: You will be responsible for providing and maintaining the contact details including the levels of authorisation that any individuals may have. Claranet will only provide any information and change requests, to those personnel in accordance with this information. These details can be maintained within Claranet Online.

Patching and upgrading



What Claranet will do

Patches to the backup platform and NOC web portal: Apply patches to the backup platform as deemed appropriate and at Claranet's discretion.

Upgrading the client software: Upgrade the client software on the platform, this will be automatically pushed to your environment.

Changes requested by you

You can update and amend your backup configuration using the local installation of the Enterprise Backup software. This includes the data that you have selected for backup, the timing and frequency for your backup, the number of generations held and the retention rules you wish to apply to the selection.

Where you require assistance with specific changes, this can be done by raising a ticket through Claranet Online. Details of how to do this can be found in the **Appendix: Help and Support**.

What you will do

Update your backup configuration: Apply changes to your service relating to the data selected as outlined in Service Overview.

Change control process: It is your responsibility to familiarise yourself with the official Claranet change control process and to follow this process every time a change to the Service is required. Details of this process can be found in **Appendix: Help and Support**.

Change request impact: It is your responsibility to ensure that any changes will not directly cause a service outage or disruption of the service.

Change of services: If you request a new service, a change of service type, or a change in service features, they must be requested via your Account Manager and may be subject to prevailing fees.

Monitoring

Once your service is up and running, Claranet will monitor your backup platform against a number of performance and availability metrics to ensure that the platform remains live.

What Claranet will do

Monitor storage averages: Monitor of storage loads and utilisation to ensure the highest performance and stability.

Pro-active alerts: Set up pro-active alerts that are in place on the platform and the storage cluster to ensure there are no bottlenecks.

What you will do

Contact support: If you experience continued loss of performance, please contact the Claranet support desk and raise a support ticket so that it can be investigated.

If a threshold is breached or a service affecting event occurs, the Claranet Operations team are notified to raise a ticket and take appropriate action to resolve the issue. This could include troubleshooting and resolving the problem, or notifying you that your backup accounts have a specific problem. There are predefined response times to event notifications that are based on the severity of the issue. These are outlined below.

What Claranet will do

Severity response times: Respond to a threshold breach depending on the severity of the breach:

Major:
Claranet will acknowledge any alarms on the system within 30 minutes

Minor:
Claranet will acknowledge any alarms on the system within 60 minutes

Warning:
Claranet will acknowledge any alarms on the system within 1 day

Change to monitoring tools: Claranet reserves the right to change its monitoring tools, methods, parameters and polling intervals over time

Help and support

Service Desk support

What Claranet will do

Support times and Service Desk: Provide support 24x7x365 once your service is up and running.

Raising tickets: Provide Claranet Online access in order for you to raise support tickets. Details of this can be found in the **Appendix: Help and Support**.

Escalation: In the event that an escalation is required, Claranet provides a clear escalation process to allow you to contact the appropriate person within the company. Details of this can be found in the **Appendix: Help and Support**.

Service Levels

The Service Level determines the metrics by which the service is deemed as operational. Details showing the expected levels can be found in the **Appendix: Service Levels**.

What Claranet will do

Metrics exceeding the thresholds: In the event that a monitored metric exceeds the acceptable thresholds, Claranet will raise a support call to investigate the incident and contact you in accordance with the escalation details held.



Appendices

Here you will find further information regarding the technical specifications of the service as well as standard procedures and agreements.

Claranet UK Data centres

The service is provided in two Claranet UK data centres at Chelmsford, Essex and Hoddesdon, Hertfordshire. The data centres meet the following specifications:

- Redundant power supplies are implemented. Hardware is connected to two separate Power Distribution Units (PDUs) and protected by dedicated UPS and generator backup
- Very Early Smoke Detection Apparatus (VESDA) is used
- A fire suppression system is installed
- Fire-retardant racks
- The environment is maintained by close-control down-flow air conditioning units that offer stable temperatures and humidity
- The data centre is manned and monitored by on-site security personnel with CCTV motion-sensitive and time-lapsed perimeter and interior monitoring

What Claranet will do

Data centre audit requests: Provide the facility for organised data centre visits. Claranet retain the right to charge for any expenses incurred during an audit visit. An audit will be defined as allowing a review and examination of systems, data security and physical security of the data centre. Any questions and names of individuals must be forwarded prior to the audit to the Account Manager assigned to you within Claranet. Claranet will specify a date and time when it is suitable for an audit to occur. This can be arranged by contacting the Account Manager.

Relocation of equipment: Be entitled, upon giving no less than three months written notice to you, to move equipment used in connection with the provision of the service between Claranet data centres within the UK. You agree to co-operate in good faith to facilitate any such relocation. Claranet shall be responsible for any costs and expenses incurred as a result of any such relocation and will use reasonable efforts to minimise and avoid any interruption to the service.

Appendix: Components

The Enterprise Backup software

The DS-Client software is installed on your environment on a server.

Hardware requirements

Minimum specification

- Virtual or Physical
- Processor:
2GHz or greater
- RAM:
4GB or more
- Hard drive space:
Minimum requirement of 2GB of storage space or more is recommended

Operating System compatibility

Table: Supported Operating Systems

Supported Operating Systems	Supported Databases
<ul style="list-style-type: none"> • Windows XP <ul style="list-style-type: none"> - Professional SP3 (x86) - Professional SP2 (x64) - Media Center SP3 (x86) - Media Center SP2 (x64) - Home SP3 (x86) 	<ul style="list-style-type: none"> • MS SQL Server 2005 Express SP4 • MS SQL Server 2008 SP3 or MS SQL Server 2008 Express SP3

Supported Operating Systems	Supported Databases
<ul style="list-style-type: none"> • Windows Vista <ul style="list-style-type: none"> - Ultimate SP2 (x86/x64) - Enterprise SP2 (x86/x64) - Home Basic SP2 (x86/x64) - Home Premium SP2 (x86/x64) - Business SP2 (x86/x64) 	<ul style="list-style-type: none"> • MS SQL Server 2005 SP4 or MS SQL Server 2005 Express SP4 (x86) • MS SQL Server 2008 SP3 / R2 SP2 or MS SQL Server 2008 Express SP3 / R2 SP2 • MS SQL Server 2012 SP1 Express
<ul style="list-style-type: none"> • Windows 2008 <ul style="list-style-type: none"> - Standard SP2 (x86/x64) / R2 SP1 (x64) - Enterprise SP2 (x86/x64) / R2 SP1 (x64) - SBS SP2 (x64) - Datacenter SP2 / R2 SP1 (x64) 	<ul style="list-style-type: none"> • MS SQL Server 2012 SP1 • MS SQL Server 2005 SP4 or MS SQL Server 2005 SP4 (x86) • MS SQL Server 2008 SP3 or MS SQL Server 2008 Express SP3 • MS SQL Server 2008 R2 SP2 or MS SQL Server 2008 Express R2 SP2
<ul style="list-style-type: none"> • Windows SBS 2011 <ul style="list-style-type: none"> - Standard (x64) 	<ul style="list-style-type: none"> • MS SQL Server 2008 R2 SP2 or MS SQL Server 2008 Express R2 SP2
<ul style="list-style-type: none"> • Windows 7 <ul style="list-style-type: none"> - Ultimate SP1 (x86/x64) - Professional SP1 (x86/x64) - Enterprise SP1 (x86/x64) 	<ul style="list-style-type: none"> • MS SQL Server 2008 R2 SP2 or MS SQL Server 2008 Express R2 SP2 • MS SQL Server 2005 SP4 or MS SQL Server Express SP4 • MS SQL Server 2008 SP3 or MS SQL Server 2005 Express SP3 • MS SQL Server 2012 SP1 or MS SQL Server 2012 SP1 Express
<ul style="list-style-type: none"> • Windows 2012 <ul style="list-style-type: none"> - Essentials (x64) - Standard (x64) - Datacenter (x64) 	<ul style="list-style-type: none"> • MS SQL Server 2012 SP1 or MS SQL Server 2012 SP1 Express • MS SQL Server 2008 SP3 / R2 / SP2 or MS SQL Server 2008 Express SP3 / R2 SP2
<ul style="list-style-type: none"> • Windows 8 <ul style="list-style-type: none"> - Pro (x86/x64) - Enterprise (x64) 	<ul style="list-style-type: none"> • MS SQL Server 2012 SP1 or MS SQL Server 2012 SP1 Express • MS SQL Server 2008 SP3 / R2 / SP2 or MS SQL Server 2008 Express SP3 / R2 SP2

Supported Operating Systems	Supported Databases
<ul style="list-style-type: none"> Novell <ul style="list-style-type: none"> Open Enterprise Server 11 (x64) 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1
<ul style="list-style-type: none"> Novell <ul style="list-style-type: none"> Open Enterprise Server 2 SP3 (x86) 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1 PostgreSQL 8.1
<ul style="list-style-type: none"> SUSE Linux <ul style="list-style-type: none"> Enterprise Server 10 SP4 (x86/x64) 	<ul style="list-style-type: none"> PostgreSQL 8.1
<ul style="list-style-type: none"> SUSE Linux <ul style="list-style-type: none"> Enterprise Server 11 SP2 (x86/x64) 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1 PostgreSQL 8.3, 9.0
<ul style="list-style-type: none"> Red Hat Linux <ul style="list-style-type: none"> RHEL 5.8, 5.9 (x86/x64) 	<ul style="list-style-type: none"> PostgreSQL 8.4 Embedded PostgreSQL 9.1
<ul style="list-style-type: none"> Red Hat Linux <ul style="list-style-type: none"> RHEL 6.2, 6.3 (x86/x64) 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1 PostgreSQL 8.4, 9.0
<ul style="list-style-type: none"> Red Hat Linux <ul style="list-style-type: none"> RHEL 6.4 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1
<ul style="list-style-type: none"> Mac OS X <ul style="list-style-type: none"> Leopard / 10.5 (PPC & Intel) 	<ul style="list-style-type: none"> PostgreSQL 8.3, 8.4
<ul style="list-style-type: none"> Mac OS X <ul style="list-style-type: none"> Lion 10.7 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1
<ul style="list-style-type: none"> Mac OS X <ul style="list-style-type: none"> Snow Leopard / 10.6 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1 PostgreSQL 8.4, 9.0
<ul style="list-style-type: none"> Mac OS X <ul style="list-style-type: none"> Mountain Lion / 10.8 	<ul style="list-style-type: none"> Embedded PostgreSQL 9.1

Appendix: Elements

Security

All customer information that is transferred to the Enterprise Backup platform is encrypted, using the encryption keys provided by you and configured during the software installation.



What you will do

Retain your encryption key: You are the only one that has access to your encryption key. Make sure that you safely record and store your encryption key. **It may not be possible to restore data without the encryption key.**

Pricing

Volume of data stored

You are charged a price per GB for the total volume of data that you have stored on the Claranet Enterprise Backup data storage platform each month. The total amount of data stored is affected by the combination of the backup parameters described previously, the number of generations you wish to keep and the retention rules you have applied. The more versions you have, the higher the total volume of stored data. The total volume of data stored for a given month is based on a usage extract taken from the platform on the first day of the following month.

Charging methods

There are two methods of contracting for the service. If at any point you wish to change the method of charging, please contact your Account Manager.



What Claranet will do

Pay as you Go: Provide a flexible approach where you pay for the total volume of stored data as outlined above at a fixed rate per GB per month. The amount each month may change as the volume of data you are storing will increase or decrease.

Monthly minimum commitment: You can commit to a minimum fixed storage level at a reduced rate. Please note that you will pay the minimum amount each month based on the agreed storage volume, regardless of whether you have utilised all of the agreed capacity or not. You are able to exceed this minimum commitment amount.

One-off setup fee

There is a small setup fee in order for us to assist you during the initial installation of the software.

Appendix: Support

Help and Support

Change Control Process

Claranet's Change Management team are responsible for requests relating to changes you wish to make. The Change Management team are responsible for Claranet's Change Advisory Board (CAB), which discusses and approves changes. To make a change request, see the section below on "Raising a support ticket".

Raising a support ticket and a Request For Change (RFC)

Claranet provides two ways for your approved contacts to raise, track and update standard support tickets; through Claranet Online and by telephone. For security and audit reasons, you are required to make all requests for change through the Claranet Online portal and only portal users with the correct privileges can request a change. You will only see your

services listed so please select the service relating to the request for change. In the event that the customer portal is unavailable, please contact Claranet by telephone, where an emergency procedure will be in place to log change requests on your behalf. Request for changes will not be accepted through this number at any other time.



What Claranet will do

Through Claranet Online: The ticket you raise is assigned to the appropriate support team based on the service you need the support for. You will only see your services listed so please select the service relating to the incident or to the service request. The response time will start from as soon as your ticket has been submitted.

By telephone: When choosing to raise a support ticket using the telephone you must provide proof of identity following Claranet's standard security procedure. The response time will start from as soon as your telephone call has ended.

Escalating a ticket

In the event that you need to escalate a ticket, Claranet is ready and available to help you quickly bring your issue to closure. Within each level of the escalation path the person you speak with is responsible for evaluating your situation, facilitating the resolution plan, and acting as your sponsor. The benefits of the escalation procedure are:

- ITIL accredited staff owning your escalation
- A focus on service recovery
- Improved communication
- Consistent process

An escalation may be initiated when, after working through our standard support processes and with our teams, you are not satisfied with the level or timeliness of the service you have received. Additionally, an escalation should be initiated when there is tangible impact to your production environment, or there is high risk to your business operations.



What Claranet will do

Escalation Manager: Assign an Escalation Manager who will deal with your escalation and collaborate with you to develop a communication plan. A technical plan of action may be needed to ensure resolution of a technical issue. Your Escalation Manager works as your advocate internally and will become a virtual member of your own problem resolution team. Should you feel dissatisfied with the escalation process, please contact your Account Manager directly.

Service Delivery – Fix levels and response times

The circumstances where a fix service level is deemed to be met are:

- When the service has been fixed within the standard and expected response time
- Where you receive a telephone call (within the service level response time) resulting in a fix over the telephone
- Where you receive a telephone call and you defer the visit of an engineer to a specific time, the fix time is measured from the specific time you specify
- Where it is subsequently discovered that the issue giving rise to the telephone call falls outside the Services agreed to be provided by Claranet
- When the equipment has been returned to an acceptable operational status or an item of loan equipment has been supplied
- Where the fault relates to an excepted Service



What you will do

Efforts to resolve an issue: You are responsible for providing support and information to Claranet in order to help in the resolution of any technical issues.

Service outage: In the event of a Service outage, you are responsible for complying as quickly as possible with any requests from Claranet for help with diagnostics. Any delay in resolving the fault due to you not being available or not complying with Claranet's requests may impact the validity of any Service Levels.

Table: Service Level Response Times

Priority	Service Level Response	Description
1 – Critical	Within 1 hour	Total service is unavailable
2 – Major	Within 2 hours	Partial service, an element of the total service has failed
3 – Minor	Within 4 hours	Impaired service, no element has totally failed but there is a quality issue
4 – Request	Within 1 Business Day	The service is unaffected. Request for product related technical advice or configuration change

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.

Measure of availability

In the event of the Service failing, we measure non-availability as Claranet being unable to back up or restore backed up files due to a malfunction of the software or the Enterprise Backup storage platform. Non-availability is calculated from the time the Service or part thereof experiences a failure until such time as the service is restored to you. Periods of Non-availability will be measured by our internal system logs.

If the Claranet monitoring system is unable to receive or process monitoring data, this shall not constitute unscheduled downtime. If you initiate a Service Credit request, Claranet will coalesce the system's monitoring data and logs with your own records of when and where an outage occurred. The Service Credits will be available for that agreed window. You have the option to dispute records with Claranet and Claranet will provide to the fullest extent permissible the system's monitoring data to you.

In the event that you and Claranet agree that Claranet has failed to meet any service level Agreement during any 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 50% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in this agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Service availability guarantee

If Claranet fails to meet the availability guarantee, Service Credits will be paid according to the table below. Only one credit may be selected and the credits are not cumulative.

Table: Service availability commitments

Percentage service availability per calendar month	Percentage credit of monthly charge for the service, for the calendar month in which non-availability occurs
Equal to or greater than 99.9%	No credit
Less than 99.9%	10%
Less than 97.0%	30%
Less than 95.0%	50%

Compensation claims

Compensation claims must be submitted, in writing (email or letter), within 30 days from the service level guarantee breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. You agree to correct problems and to attempt to minimise the recurrence of problems for which you are responsible that may prevent Claranet from meeting the service level guarantees. 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 items:

- 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 Claranet on behalf of a customer;
- 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 the 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 the request of a customer;
- in the event that the Service is unavailable due 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 or others 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 failure to provide local access to facilities; 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 the technical contact details.

Limitations of use

What you will do

Use of the software: Agree to use the Asigra software in executable code only, subject to the Asigra “Software License Agreement”.

Transfer or amendment of the software: Agree not to copy, modify, adapt, alter, translate, or create derivative works from the software or the NOC web portal, merge the software or the NOC web portal with other software; distribute, sublicense, lease, rent, loan, or otherwise transfer the Asigra Software or the NOC web portal to any third party; or reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code for the software or the NOC portal.
