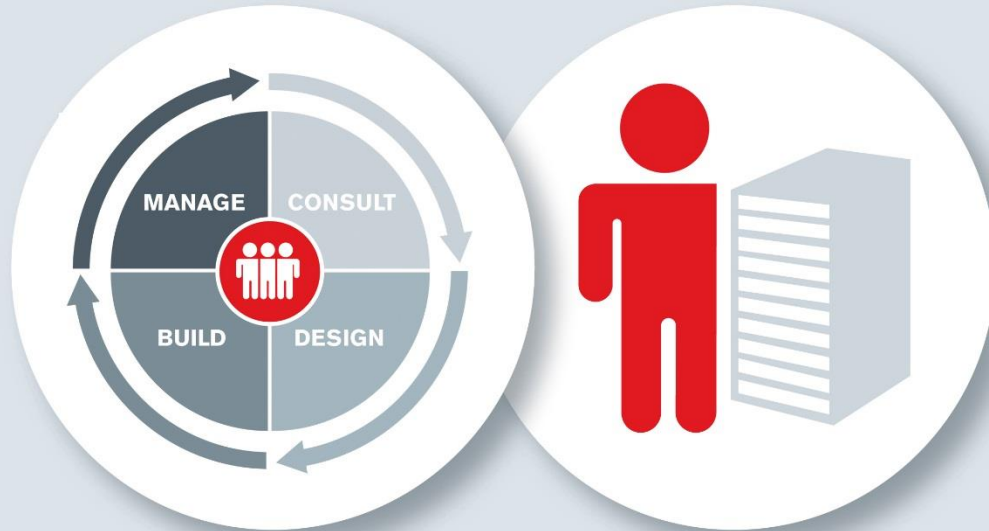


Claranet Service Description



Business Backup

Business Backup is a remote data backup service enabling you to back up data from your devices to a secure platform in a UK-based Claranet Data Centre.

Version 11.2

Contents

Service overview	2
Options	2
Consult	4
High Level Options Analysis	4
Packaged Consulting	4
Consulting	5
Design	6
Backup and recovery sales specialist	6
Specialist solution design	6
Build	7
Specialist engineering	8
Project Management	8
Manage	9
In-Life Management	9
Help and support	11
Service Levels	11
Appendices	12
Claranet UK Data centres	12
Appendix: Options	12
Server Edition	12
Desktop Edition	14
Appendix: Elements	15
Security	15
Pricing	15
Appendix: Support	15
Help and Support	15
Service Levels	17

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

Data loss occurs all the time, so backing up your most critical data is vital for your business. The objective is simple; to retain a copy of your selected data away from your main environment so that if the original can no longer be used, the copy can act as a replacement and you can continue with business as usual. Claranet's Business Backup powered by Data Deposit Box provides you with the protection you need, whether you are running a small or medium-sized business or a small office at home.

The Business Backup powered by Data Deposit Box (DDB) is a remote data backup service enabling you to back up data from your devices to a secure platform in a UK-based Claranet Data Centre and retrieve the data from anywhere across the internet.

There are a number of aspects within the overall backup and recovery service from installation through to the recovery of data. An outline of these can be found below and further details of each one can be found in the appropriate section within the Service Description. The Business Backup powered by DDB is a self-service offering, which means you will be able to setup and configure the solution to suit your needs.

Installation

An invitation link is sent to you via a link allowing you to log on to the Claranet Business Backup web portal, create a secure password and download the appropriate software to your devices. Installation is made easy using a short wizard.

Configuration

You are able to select the data and folders you wish to back up, specify the number of versions you wish to retain and create a schedule for your backup. This same interface allows you to add devices at any point, as well as make any changes you require.

Backup

At the time of your backup, a copy is encrypted at source and sent securely across the internet to Claranet's Business Backup platform housed in Claranet's Chelmsford data centre. The initial backup takes a full copy of the selected files and incremental copies thereafter. This means that the first backup will take longer. To see the current backup status of each of your devices, you can simply log into your account.

Recovery

You are able to initiate restoration of your files from the portal without recourse to Claranet. A secure copy of your file(s) is retrieved from the data centre and made accessible via the portal for you to download to any of your devices. 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. This service is not a Disaster Recovery solution, though Claranet can offer Disaster Recovery services as part of a full business continuity plan within your organisation if needed.

Options

The solution works in a number of different environments and you can install the software on an unlimited number of devices as a single user. This allows you to retain control of multiple devices from a single interface.

Server Edition: Microsoft Windows Server

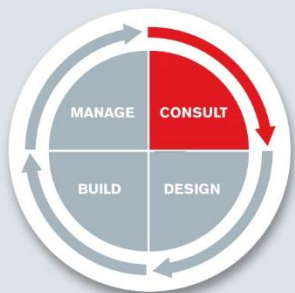
Where you are backing up a business environment which uses a server based operating system, you use the Server Edition. This “agentless” version allows you to install a single software client on to your environment without the need to install a separate client onto every physical or virtual server on the same network. Full details of the Server Edition and the various operating systems supported can be found in the Appendix: Options.

Desktop Edition: Microsoft Windows PC or Apple environment

Where you are backing up an individual PC or Apple running an individual desktop based operating system, you use the Desktop Edition. Full details of the Desktop Edition and the various operating systems supported can be found in the Appendix: Options.

Customer account

Multiple devices can be set up from a single account.



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. In many cases, Claranet’s Business Backup solution may be part of a larger solution involving the Managed Hosting services or one of the Connectivity services or both.

Depending on the complexity of requirements, one or more workshops between you and Claranet may be arranged in order to outline your requirements. These may be conducted by Solutions Consultants, Strategy Consultants, Solutions Architects and Enterprise Architects who will be applied at our discretion. It is in everyone’s interests to ensure that the proposed solution will meet your requirements and one of our first roles is to focus on your business, your IT requirements and to produce a high level scoping report, the High Level Options Analysis. This will allow you to make an informed choice as to the recommended path.

High Level Options Analysis



What Claranet will do

Deliverable: The High Level Options Analysis report. A short, high-level scoping document.

Time to complete: The High Level Options Analysis is a consulting based service and is included up to a maximum of 2 days work at Claranet’s discretion. In some instances, the work required to produce a High Level Options Analysis could extend beyond this e.g. where the requirements need extensive discussion or the options are particularly complex. If this is the case, Claranet will agree with you a charge for the additional work required to produce a High Level Options Analysis to establish the requirement.



What Claranet will do

Technical Design: Technical work beyond this falls outside of the scope of the High Level Options Analysis and is carried out in the Design phase.

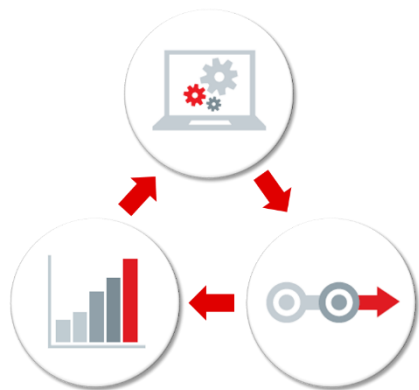


What you will do

Information sharing: Provide any requested information to allow Claranet to deliver a High Level Options Analysis. This will include full details of on-going technical contacts within your organisation. This information will form the basis of the Initial Configuration, so it is your responsibility to ensure the information provided is correct.

Packaged Consulting

Claranet has a number of pre-packaged assessments and audits that help to outline your readiness in respect of particular IT options. It may be that the completion of one or more of these packaged consultancy engagements is made as a result of the recommendations made in the High Level Options Analysis report. 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

Assessment options:

- Linux Infrastructure Maturity Assessment (LIMA)
- Infrastructure Maturity Assessment (IMA)
- Cloud Readiness Assessment
- Open Source Assessment

Pricing: This additional packaged consulting service is optional and is a chargeable event. Claranet provides three prices for each assessment depending on the size of your company and the complexity of your requirements: Small / Medium / Large.

Consulting

A packaged consulting approach can be of significant help to many organisations. However, Claranet also provide a specialist consulting service that can be used at any time (including pre-contract) to help you in areas outside of the packaged offering. This engagement is specific to you and can cover any area that is needed with regard to your business and technology.



What Claranet will do

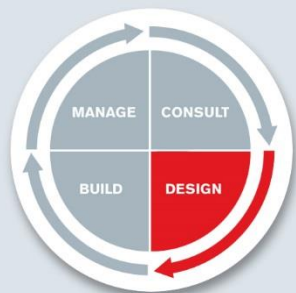
Specialist consulting: Provide a range of specialist expertise in a variety of areas. This includes a detailed focus on your business in order to ascertain the scoping requirement or where you are unsure as to the direction your business should take in the ever-changing IT environment.

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

Pricing: This additional consulting service is optional and is a chargeable event and is based on a consultancy day rate.

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

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



Design

Your Claranet Business Backup 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.

Claranet will undertake to identify which elements and options are required and how they should be configured to meet your requirements. Your solution may require the utilisation of a Solution Architect and if so, the output of this process is a proposal document and a Statement of Works (SoW). It may be part of a larger document if the Business 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. However, fully specifying a complex complete new hosting infrastructure is not part of the standard design work. If this is required at this stage, it can be completed using Claranet's Specialist Solution Design service.

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 and recovery sales specialist

As part of your standard Managed Hosting Service, Claranet provides a Backup and Recovery sales specialists 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 also to help ensure that the proposed technical solution will fit your business and achieve the outcomes you are looking for.

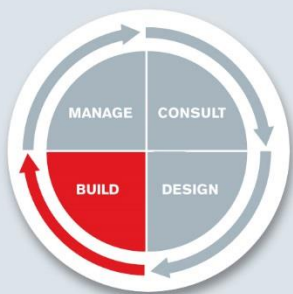
Specialist solution design

At times, the complexity of your solution design will require additional or specialist design work in order to detail your requirements.

What Claranet will do

Specialist level of design work: Produce technical design work on your proposed solution in order to specify your requirements fully. This may be completed by a Solutions Architect or a Claranet Technical Specialist in that particular field.

Pricing: This additional specialist solution design service is optional and is a chargeable event and is based on a day rate for the service.



Build

Once your order has been placed, Claranet will advise on installation and configuration activities to ensure a copy of your data is stored in the Claranet data centre.

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

Installation

What Claranet will do

Account creation: Create an individual account on the backup platform for you once you have signed up for the service.

Invitation link: Provide an invitation link to the Claranet Business Backup web portal so you can download the software and install on to your device: (<https://mydata.ddbcloudbackup.com/>)

What you will do

Invitation link and password: When connecting to the portal, you will create a secure password as part of your login. If you lose your password, a reset password option is available.

Download and installation: Log into the web portal and download the required software onto your machine. Installation is with a short wizard.

Internet connection: Ensure that all devices have access to the internet in order to successfully complete backups.

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

Configuration

What you will do

Data selection at installation: Part of the installation will initially select "My Documents"; "Desktop" "IE Favourites" and "Windows Mail" folders for backup though these can be deselected. If any folder is selected, any corresponding sub-folders are automatically selected.

Data selection with Server Edition: By drilling down through your folders and sub-folders you can select individual files to be backed up. The service can protect all areas of your business, including:

- Files
- Folders
- Microsoft Exchange
- Microsoft SQL
- SharePoint

Any file selections can be easily changed using the same interface in the portal.

Data selection with Desktop Edition: After the installation, you can easily select files and folders to back up using the portal.

Although the service is installed, configured and managed by you, Claranet may provide necessary engineering and project co-ordination in order to assist in the delivery of your solution. Depending on scale, this may involve engineering support as well as a Project Co-ordinator who will guide your project from implementation through to set up. There are a number of steps that need to be followed and our support teams are there to ensure it goes smoothly.



What Claranet will do

Additional tasks: Perform additional tasks outside those described and as part of the service elsewhere in the document. There is an additional charge for the engineering time incurred to perform these tasks. Any requirements in addition to those agreed in the order may be able to be fulfilled; however, this will also have an impact on the implementation time frame. Claranet reserves the right to charge on a time and materials basis for any additional work.

Specialist engineering

It may be that your particular setup requires additional specialist engineering work. This will be quoted individually and could include specialist change requests, work on piloting projects or prototyping.



What Claranet will do

Specialist engineering: Provide a quotation for specialist engineering work based on a day rate.

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 Account Manager, the Solution Architect and Project Co-ordinator who are 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.



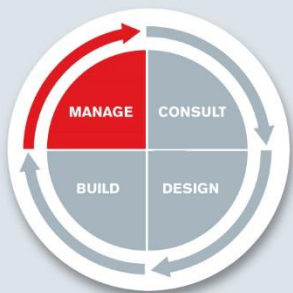
What Claranet will do

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.

Acceptance procedure

Once the backup service is setup and connected, the ongoing management is under the process of the In-Life Management process.



Manage

Your solution is managed In-Life by our Service Operations team who provide a pro-active, ITIL aligned service. You also have access to your Claranet Business Backup web portal.

In-Life Management

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 and operational within the Service Levels.

Backup

With the initial backup, a full copy of the selected files is taken and encrypted using 448-bit military grade encryption whilst they remain on your machine. These files are then sent securely across the internet or network to Claranet's Data Deposit Backup platform in our data centre in Chelmsford, Essex. The initial backup will take longer than future backups which are incremental and take a copy of only those parts of the files that have changed or a copy any new files that have been added. The smaller incremental backups are stored separate to the original allowing you to restore earlier versions of your files.

Data recovery and restoring files

In the event of data loss you initiate restoring either an individual file or the total files that are backed up by logging on to the web portal and selecting the "My Files" option. A secure copy of your file(s) is retrieved from the data centre and made accessible through the portal for you to download to any of your devices.

Your file is decrypted within the system and made available for download as part of your download queue. Any files that you have added to your download queue that you have not downloaded will be automatically removed after 7 days. To access your download queue, you can navigate to My Downloads. You can select individual or multiple files and folders for restoration. Multiple files and folders will be zipped into one file before you download them.

What you will do

Backup and recovery selection: You will be responsible for adding and removing files and folders from your backup selection.

Backup and recovery completion: You will be responsible for ensuring that the backups are successful and that you can access and restore your data from the web portal.

Restoring data: You will be responsible for accessing and restoring your data from the web portal.

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 utilization. It may be necessary to make changes **without** prior notification to ensure the continued operation of the managed service.

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

Upgrading the client software: Upgrade the client software which will be automatically pushed to your device.

Changes requested by you

Claranet's Business Backup is a self-service offering once your initial account has been set up. Through the web portal you can update and amend the parameters on each of your individual backup accounts. This includes the timing schedule, the number of generations

held and the data selected for backup. You can also add, edit and delete users as well as amend the total backup storage that has been allocated.

Where you require specific changes to be made or wish to request a help desk ticket, these can be made by raising a ticket through Claranet Online and details of how to do this can be found in the **Appendix: Help and Support**.

What you will do

Self service: Make all changes to the backup accounts relating to data selected, schedule, new users and devices.

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 other 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.

When a threshold is breached

What Claranet will do

Monitor storage averages: Monitor of storage cluster loads and utilization to ensure the highest performance and stability of the cluster

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

What you will do

Contact support: If you do 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 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: Reserve 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 the Business Backup service has been set up.

Raising tickets: Changes to your service configuration can be made through the Claranet Online ticket request and 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 parameters by which the service is accountable. Details of the metrics showing the expected service levels can be found in the **Appendix: Service Levels**.



What Claranet will do

Information delivery: Obtain the results for each of the metrics and contact you according to your list of authorised contacts in the event that any results fall outside of the acceptable parameters.

Archiving results: Retain an archive version of the monitoring results for up to 90 days which can be available to you on request through the Claranet Online portal.

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 services are provided Claranet's UK data centre at Chelmsford, Essex. This data centre meets 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
- All components are fire-retardant including racks, cables and cable management
- 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: Options

Server Edition

Hardware requirements

Minimum hardware requirements for devices

- Processor:
Pentium 4 @ 1.7 GHz,
- RAM:
512 MB minimum, 1 GB recommended
- Hard drive space:
Minimum requirement of 5GB of storage space is recommended

Operating Systems compatibility

Table: Supported Operating Systems

Server Edition supported Operating Systems

- Windows XP Professional SP2;
 - Media Center SP2
- Windows Vista Business SP1
 - Ultimate SP1
 - Enterprise SP1
- Windows 2003/2008/2008 R2 2012 2012 R2
 - Standard SP1
 - Enterprise SP1
 - SBS SP1
- Windows 7 Professional
 - Enterprise
 - Ultimate
- Windows 8 Basic
 - Professional
 - Enterprise
- Windows 10
 - Home
 - Pro
 - Enterprise

Backup protection

The Server Edition allows full scheduled backups to be implemented.

What you will do

Scheduled backups: Allow multiple backup schedules to be set up, each with a different data set. These will be allocated a time for backup

File selection: All files and folders can be selected or deselected individually.

No of generations retained: Retain a default of 14 generations of files. You can amend this to retain as many file generations as wished.

Web portal and connectivity

What Claranet will do

Web portal: Provide access to your account through the Business Backup web portal.

Firewall compatibility: Ensure the software is compatible with the majority of home and office hardware firewalls.

What you will do

Browser compatibility: Ensure that a suitable browser is installed in order to access the web portal. The 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

Desktop Edition

Hardware requirements

Minimum hardware requirements for devices

- Processor:
2 dual CPU 2.0GHZ
- RAM:
<1M files 3GB; > 2M files + 4GB
- Hard drive space
A minimum requirement of 1GB of storage space is recommended but is purely based on usage patterns

Operating Systems compatibility

Table: Supported Operating Systems

Desktop Edition supported Operating Systems

- Windows XP Professional SP2
 - Media Center SP2
- Windows Vista Business SP1
 - Ultimate SP1 and Enterprise SP1
- Windows 7 Professional
 - Enterprise
- Ultimate Windows 8 Basic
 - Professional
 - Enterprise
- Windows 10 Home
 - Pro
 - Enterprise
- Mac OS:
 - X Leopard 10.7 or above

Backup protection

The Desktop Edition provides a Continuous Data Protection (CDP) method of data protection.

What you will do

Continuous Data Protection (CDP): Provide the Continuous Data Protection facility with the Microsoft Windows PC and Mac versions of the software. 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 Business Backup platform at Claranet's data centre in Chelmsford, Essex.

File selection: Provide data selection based on individual folders. It is not possible to select individual files within a folder with the Desktop Edition option.

No of generations retained: retain up to 64 generations of an individual file. The Business Backup service will discard earlier generations automatically.

Web portal and connectivity

What Claranet will do

Web portal: Provide access to your account through the Business Backup web portal.

Firewall compatibility: Ensure the software is compatible with the majority of home and office hardware firewalls.

What you will do

Browser compatibility: Ensure that a suitable browser is installed in order to access the web portal. The 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

Appendix: Elements

Security



What Claranet will do

Encryption: Encrypts and protects your data using military-grade 448-bit “blowfish” encryption. This uses a system defined key to encrypt your data before it leaves your device and stores it as encrypted data on the Business Backup storage platform at Claranet’s data centre. The encryption key is retained on the storage platform having been encrypted with an internal “RSA algorithm”.

Access to your data: Deny access to your data and to the encryption keys to all those without authorised access. This includes Claranet personnel. Claranet has **no** access to the data nor to the encryption keys.

Pricing

Volume of data stored

Charging for the service is straightforward. You are charged a price per GB for the average volume of data that you have stored on the Claranet Business Backup data storage platform during the month across all of your devices. The average amount is based on the daily stored total, divided by the number of days in the calendar month.

There is no initial setup fee or licence fee. The amount of data stored is affected by the number of generations of a file that you wish to keep. The more versions you have, the higher the volume of stored data. You can view your storage consumption at any point from the Business backup portal.

Charging methods

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



What Claranet will do

Pay as you Go: Provide a flexible approach where you pay for the volume of data as outlined above at a fixed rate per GB per month.

Monthly minimum commitment: Provide an alternative method of charging to introduce a reduced rate per GB per month. You can commit to a minimum fixed storage level at a reduced rate per GB as well as being able to exceed this amount should you need to. Please note that you will pay the minimum amount each month based on the agreed storage level, regardless of any unused storage you have between the actual volume of data stored and the agreed storage level.

Appendix: Support

Help and Support

Change Control Process

Claranet’s Change Management team are responsible for requests relating to any product and service configuration changes you wish to make that can’t be made through the web portal. The team specialise in configuration and follow strict processes and ensuring that the changes are authorised. The Change Management team are also responsible for Claranet’s Change Advisory Board (CAB), which discusses and approves changes raised internally. 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 most efficient way of raising support tickets is through the Claranet Online portal. 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 reasonable efforts support and information to Claranet 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 follows:

Not being able to back up, access or share files due to a malfunction of the software or the Business Backup storage platform.

Non-availability is calculated from the time the service or part thereof experiences a failure to such time as the service is restored to you. Periods of Non-availability for the Business Backup platform will be measured by our internal system logs

Any time in which the Claranet monitoring system is unable to receive or process monitoring data shall not be assumed to be unscheduled downtime. If you initiate a Service Credit request, this will put into a process where Claranet coalesce the systems monitoring data and logs with your own record 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, where upon systems monitoring data can be provided to you.

In the event that you and Claranet agree that Claranet has failed to meet any service level guarantee 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 to any failure local access 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 the technical contact details.

Limitations of use

What you will do

Use of the software: Agree to use the software in executable code only, solely via a download from the Business Backup powered by Data Deposit Box web portal and solely as part of the service, subject to the Data Deposit Box End User Licence Agreement.

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

Liability: Agree not to make Claranet liable for any consequential, indirect, punitive, exemplary, special or incidental damages, including any lost data and lost profits arising from or relating to this agreement.

Third-party Contract Termination

In the event of the termination of a contract for services by Claranet of a third party supplier that is required to deliver the Services, Claranet will apply commercially reasonable endeavours to migrate your backup account to another materially equivalent Claranet service. You will be notified at least 30 calendar days before any potential migration by Claranet of your backup account. Claranet will run both backup services in parallel for a maximum of 30 calendar days from the date of the migration therefore allowing 30 calendar days of changes to be stored at the alternative backup platform before the previous backup account is decommissioned.