Arkivum
Every bit archived

ArkivumLimited
R21 Langley Park Way
Chippenham
Wiltshire
SN15 1GE
UK

+44 1249 405060

info@arkivum.com
@Arkivum
arkivum.com

Frequently Asked Questions (FAQs)

Table of Contents

Title
Arkivum Frequently Asked Questions (FAQs)

Part no
ARK/BN/ALL/0145

Version
2.0

Date
5 Oct 2013

Status
Release

Introduction

This FAQ has been written to help answer the common questions that both current and prospective clients of the Arkivum service raise. It has been deliberately written to provide transparency of the service, in plain English, and without assuming that the reader is an expert in either Archiving or Information Technology.

The FAQ is organised into the following sections:

- Legal and Contractual
- Security
- Support
- Management
- Using the Service
- Integration

Naturally, the list of questions and answers is not exhaustive. Should you have any new questions or suggestions for improvements, then we would be delighted to receive your comments.

Legal and Contractual

How can you offer a 100% guarantee?

Arkivum believes that it is providing a market leading service and uniquely offers you a 100% data integrity guarantee.

To do this we follow industry best practice and take additional steps to keep the likelihood of any data loss to an absolute minimum.

We are so confident in this that in the event of a data loss, we provide a financial guarantee underwritten by an insurance policy, which means that you would be covered for direct losses relating to that data loss.

This means we have no loopholes to allow us to void our commitment to you and the integrity of your data. How many other vendors can say that?

Who owns the data in the archive?

You own your data. The data is encrypted at inception into our systems and cannot be viewed by us. Your information remains this way until you retrieve your information back from our system and enter the encryption key which only you have access to.

Who owns the Escrow tapes that store my data?

Please see the terms and conditions for the escrow agreement in the service contract.

If you do not currently have a copy of this, please contact us by e-mail at info@arkivum.com where we will be happy to provide a copy of the terms and conditions of service.

How/when do I get access to my Escrow tapes?

Please see the terms and conditions for the Escrow agreement in the service contract.

If you do not currently have a copy of this, please contact us by e-mail at info@arkivum.com where we will be happy to provide a copy of the terms and conditions of service.

What is your Service Level Agreement (SLA) for availability of the service?

The SLA defines our contractual service agreement regarding service levels to our clients. We detail how we provide a service level that covers the Uptime Service Availability, Data Safety and Data Retrieval. For example:

- We will ensure that the Storage Services are available at least 99.9% of the time.
- When a client retrieves files from the service, we will ensure that the files are bit-for-bit identical to the file as originally provided by the client and will demonstrate this through use of checksums.
- We will ensure that the time to begin transferring a file from the Storage Services to the client's network does not exceed 5 minutes (the "Latency Service Level").

If we do not meet these Service levels then we will typically pay a service credit. For more details please see the terms and conditions regarding SLA availability in the service contract. If you do not currently have a copy of this, please contact us by e-mail at info@arkivum.com where we will be happy to provide a copy of the terms and conditions of service.

Is the service available via G-Cloud?

Yes. Arkivum's service is available from the UK Government's CloudStore. See http://govstore.service.gov.uk/cloudstore/search/?q=arkivum

How much does the service cost?

Costs are tailored to the client service. Prices start at GBP 1000 per Terabyte* per year and decrease to GBP 360 per Terabyte* per year, dependent upon data volumes. Further discounts are available for multi-year education clients, longer term storage commitments and "lifetime" contracts.

For further details please speak to a member of our sales team, or e-mail info@arkivum.com

*1 Terabyte = 1TB = 10^{12} Bytes

What Is OSCAR?

OSCAR is a complete on-site archive storage solution that is delivered to the client's site and, where appropriate, fully managed by Arkivum.

OSCAR utilises all of Arkivum's long term retention policies and procedures to deliver an out of the box solution to long term, on-site, archive storage.

Is there a difference in costs for OSCAR?

Arkivum's service includes the long-term total cost of data retention and access (staff, equipment, hosting, network, migrations and upgrades, integrity audits, escrow etc.). Not all of these are included in the in-house service, e.g. the costs of power, cooling, space etc. will be borne by the customer. Arkivum can provide remote monitoring and management of the on-site system and will handle maintenance, upgrades and migrations. This means comparing the cost of an in-house vs external service has to be done in a way that makes sure all costs are fully accounted for in an in-

house deployment. It is important to do this over the full retention period for the data being stored, e.g. 10 or 20 years. The price of the on-site system will also vary depending on the capacity needed, the amount of disk cache, and whether multiple on-site copies of the data is needed. Arkivum is happy to provide specific quotes for OSCAR on request.

Under what conditions do you pay out for data loss?

In the most extreme circumstance, in which Arkivum loses vital data from our 3 data storage locations, then you will be protected against direct loss which is measurable and renewable up to GBP 5 million, with worldwide cover. This financial guarantee is underwritten by an Information and Communication Technology Professional Liability Insurance Policy.

There are limitations on this financial guarantee, set out in our contracts including matters outside our control or indirect or consequential loss. A theoretical case study provides further details in Appendix A.

Security and Compliance

Where is my data stored?

Your data is stored in three pre-defined locations, which are agreed with you when you sign up to the service. These include a primary and secondary data centre in your chosen geographical region and an agreed secure escrow provider.

The location of your data is important for security. Knowing where your data is stored at any time means you can be confident of its safe custody.

Furthermore different geographical regions have different rules and regulations surrounding computer data, which can affect not only data generated in these locations but also data stored in these countries (for example the US Patriot Act).

For those instances where data must stay on site, within a restricted network or where a client wishes to run an in-house solution Arkivum offers OSCAR, its On-Site Cloud Archive (see the FAQ What Is OSCAR?).

How secure are your secure storage locations?

Our secure storage locations are based in highly secure facilities, with our operations at all sites certified to ISO 27001 standards. Our locations are manned at all hours and access is strictly restricted to a list of named, trained and vetted members of the Arkivum Operations team. Each site is protected by best of breed firewall technology ensuring that our locations are protected from the latest advanced evasion techniques utilised by sophisticated hackers and intelligence organisations.

Are your data centres on the JANET and/or N3 networks?

We are in the process of moving to a JANET connected Data Centre (DC) for one of our data centres which will have two gigabit JANET connectivity to our server. This will be completed and operational by the end of 2013. This DC will shortly be getting N3 connectivity

For University and NHS customers, this will be their 'primary DC' so that data transferred to and from our service will all go over JANET or N3. Replication of data to our other DC (the 'secondary DC') will happen automatically through a 'DC to DC' transfer with no additional use of the customer's JANET or N3 bandwidth.

Are my data tapes shared with anyone else?

No, some storage providers share media and use de-duplication technologies which mean that they may not provide total separation of your data from that of other clients. This lack of separation increases the risks that your data could accidentally end up with another party through human or system errors or other factors.

In the Arkivum Service, your data is kept separately from other users' data through the use of dedicated media sets for each client.

This separation extends to separate media sets at each of your data centre locations and also for the media held in escrow, thus providing you piece of mind that you know where you data is at all times.

What encryption do you use?

For encryption, the centre of Arkivum's security model is the ability to separately encrypt each file stored in our service. Each file is encrypted with a unique symmetric key using AES256 encryption with the key generated from a pseudo-random seed. The symmetric key for the file is then encrypted using a public key from a public-private key pair using RSA2048 encryption. Both AES256 and RSA2048 are industry standard encryption algorithms and widely used in high security applications, e.g. electronic commerce and for sensitive government information.

The user of our service must supply the public-private key pair that is then stored in a secure keystore on the Arkivum appliance. The public key is used on the appliance to encrypt data before it enters our service and the private key is used to decrypt data retrieved from our service.

Only encrypted data is ever stored in our service. The user public-private key pair is not stored in our service so that Arkivum has no way to decrypt any user data. It is up to the user to protect the key pair that they use, e.g. by backing it up to their own safe storage. If the key pair is lost then the user's data can no longer be decrypted so it is essential that the key pair is kept safe. Arkivum can supply information on best practice key management and the third-party suppliers able to offer key storage services.

There can be a key-pair per file, key-pair per directory or simply one key-pair for all data stored in the service. Our implementation of AES encryption provides encryption of data stored on the client A-Stor appliance, whilst being sent to our secure storage locations and also within the Arkivum Data Store; this ensures that data is protected from unauthorized access both in transit and at rest.

How do you deal with file attributes and permissions for files?

File permissions and extended attributes are used to control what actions can be carried out on a file and by whom. They can also be used to store additional file information, for example the date a file was created or who last amended the file.

In the Arkivum assured archive service, permissions and attributes are stored with the archived files. These permissions are permanent and help to prove the provenance of the file. When restored, a file will have the permissions that were applied at the time it was written into the archive. This ensures that the same users will be able to read the files before and after they have been archived. However your data administrator is always able to override the permissions and access files whose rights are no longer relevant.

Can I give someone else access to my data?

Controlling access to your data is an important consideration for any company, be that preventing unauthorised access to the data or managing how to share that data with selected partners.

In the Arkivum Assured Archive, you control the encryption keys for your data, which means you retain control of who has access to it. This control ensures that nobody, not even Arkivum, can view your files and data without your explicit permission.

To allow another division of your organisation or a third party to access your data they can be provided with an encryption key and appliance that can be configured to either access your entire archive or simply small portions of it as required.

Is Active Directory supported?

Active directory and similar directory systems allow the use of a single centralised set of users and passwords. This provides for a greatly simplified and centralised management and increased security.

The Arkivum service supports Active Directory and can connect as a domain member to take advantage of your existing infrastructure.

This allows the simple control of user permissions for archived files by utilising your centralised domain users and groups.

How can I ensure that only certain groups of people have access to parts of my archive data?

To further increase security our service also offers the ability to use separate encryption keys for different segments of the archive, allowing improved control of sensitive data for which access which must be restricted of group of approved or trusted individuals, for example different divisions or departments of an organization would be physically unable to decrypt another section's data.

How do I know my unwanted data has been deleted?

Data deletion can be particularly important for compliance driven organisations, where data must only be held for a set time period.

In the Arkivum Archive, when a user deletes data, all secondary encryption keys for that data are purged ensuring that even with access to the master encryption key, the deleted data cannot be read.

The next step in the process is to remove the encrypted data from the media itself. This is carried out by issuing a file system delete for the media.

Finally when tapes are taken out of service, a secure erase is carried out making sure that the media has no data remaining on it.

If required, additional steps can be specified including a secure wipe on every deletion from the archive, secure destruction of tapes and even the return of used tapes to the client for their own secure storage or destruction when they are no longer used as part of a client's archive set.

Have you been audited? Can I audit your premises and processes?

Arkivum is ISO27001 certified and is regularly audited by external auditors.

We welcome client audits.

Is your service IL2 or IL3?

IL2 and IL3 are UK Government Information Levels. These define the sensitivity of the data stored and the security procedures and processes that need to be followed when transmitting and storing this data.

Arkivum currently has ISO27001 certified processes in place, which will meet the requirements set out for various Information Levels.

We are happy to work with providers to integrate our services to complement their IL certified offerings or to operate from IL certified data centres.

We support IL0, IL1 and IL2, with formal accreditation for these levels pending. Should you require a higher level (IL3 and IL4) then please contact us.

What about PCA, NHS IGSoC and PSN compliance?

Arkivum has satisfactorily completed the NHS Information Governance (IG) Toolkit to Level 3.

Arkivum is in the process of gaining PCA accreditation and PSN compliance.

Does the service provide an audit trail?

Yes. We recognise that customers in highly regulated sectors, for example life sciences where Arkivum stores clinical trials and medical data, strong audit trail support is essential. Audit trails from the service are made available to you to give you assurance that correct processes are being followed and to allow you to meet the compliance requirements.

How does Arkivum support 21CFR Part 11 compliance?

Part 11 of the Code of Federal Regulations deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records (Title 21CFR Part 11 Section 11.1 (a)).

This is an important standard for the Life Sciences sector. Arkivum can be instrumental in helping a company achieve 21CFR Part 11 compliance. Arkivum's service meets the key requirements of 21CFR11: Integrity, authenticity, confidentiality and the need for availability (ready access).

We have designed our system from the ground up with information security in mind. We have been certified to ISO27001, which includes a detailed risk assessment of the integrity, availability and confidentiality of client assets in our possession.

This all means that Arkivum's A-Stor service or OSCAR on-site solution can substantially reduce the cost and effort of meeting compliance. We are very transparent in what we do – you need to know that your data is safe in our hands.

We share details of our people, processes and infrastructure with both clients and auditors and we are willing to be audited when a client is itself being 21CFR Part 11 audited.

Further details on how we support 21CFR Part 11, are available in a white paper which details our approach and how we support it. Please contact us to obtain a copy of this paper.

Support

How are new releases of the service or software undertaken?

At Arkivum our team of developers are constantly adding features to A-Stor. These software updates are automatically published and notified to the user via A-Stor's administration console.

The A-Stor administrator utilises a simple mouse click to apply the update immediately or can defer the update to be applied during a maintenance window.

How do I get support if something goes wrong?

We are committed to minimising any business impact that such issues may have on our clients' day to day business operations.

Arkivum provides a transparent and simple to access support process to help us achieve our 100% data guarantee. We aim to ensure that support is provided pro-actively and that our partners and clients can utilise our support team's preservation and storage knowledge.

We also offer our partners training to provide the first level of support directly from your account management team. Our partners have direct access to Arkivum's support and development teams who will resolve any issues you may be experiencing quickly and efficiently.

Please see our support documentation for further details of this process including standard support hours and our service level agreements.

What happens if my appliance has a fault or failure?

Hardware and software faults and failures are part of everyday life when running IT services and infrastructure.

To assist in managing this, all of our hardware appliances have been designed to offer industry standard fault resilience and come with a three year, four hour, on-site warranty. During this time, failed parts will be replaced under this warranty.

Should the system undergo total failure or be destroyed (such as in a fire), a new system can be configured and archived data will still be available. In this event, the client will need to provide their encryption keys to the replacement gateway appliance before data can be accessed.

Management

How do I know my data is being stored safely?

As your data is verified and replicated to our ISO27001 certified data centres and escrow centre's system each files status will move from red, through amber to green.

Once a file is shown as green, this means that it is replicated at all three of our sites and all processes are in place to maintain that file over the length of your contract. Additionally once in this state, the Arkivum 100% guarantee applies to the file.

The status of a file can be checked at any time through the web interface, the developer API or by viewing the files extended attributes.

How do I stop my users deleting their data?

The A-Stor gateway can be configured to only allow data deletion through the administrative web interface. This ensures that in day to day use a file cannot be deleted from the system and enables an organisation to carry out any processes required to approve data deletion before being actioned.

Additionally, as the administrative interface is protected by authentication, which can be linked to your Active Directory, users' actions can be tracked through standard logging systems.

What key management do you provide?

To protect your data, Arkivum uses a unique key for every file, which is then stored in a protected key store. This key store can be considered a safe, which contains many keys, but can only be opened with a master key.

This master key is only held by you, the client. Arkivum never has access to these keys and is therefore unable to manage these keys for you.

Without the master key, there is absolutely no way in which the original data can be recovered; so it is vital that you take suitable steps to ensure that these keys are stored safely so that they can be accessed in the event of a failure, disaster or similar.

Arkivum is happy to direct you to examples of best practice or refer you to a Third Party that offers key management service. Arkivum does not offer these services directly.

Can I control who can use the service within my organisation?

Yes. The administrative interfaces and data shares are protected by user level authentication, which can be integrated with existing Active Directory infrastructure.

This means you have the same controls over who can access archived data, as you have over any other windows drive or network share.

In addition to this, where particularly sensitive data is being stored, different keys can be used to protect this, such that it can only be read by a trusted set of staff who have access to this key.

Using the Service

How do I get started?

You will need 3 elements:

1. A gateway appliance to locally hold your data and then encrypt it.
2. A service agreement (contract) to allow you to use the service. This defines how much data you can store and the costs for this storage.
3. Access to the Internet, to allow the gateway appliance to send data to our storage facilities.

How long does it take to start using the service?

Once you have signed the services contract, it typically takes 2 days for the Arkivum service to start archiving your data. The time to complete the archiving depends upon the amount of data to be archived and the speed of your communications.

What if I have a lot of data to archive in one go? How do I do a bulk ingest of data?

Arkivum offers a variety of methods for the archive of large amounts of existing data into the service. Options range from Arkivum visiting your site to collect data, so that it can be directly ingested into the service, to receiving a hard drive or tapes couriered to our offices. For further details please contact us to discuss an option that best suits your requirements.

This can be done either by calling 01249 405060 and asking to speak to a consultant or by sending an e-mail to info@arkivum.com.

How do I send data to the archive?

The Arkivum Assured Archive service is accessed through an on-site gateway appliance.

This presents the Archive as a windows share or network file system and enables files to be copied into the archive in the same way you would copy them to any other drive or share.

In addition to this method:

- the appliance also provides a web interface, where files can be uploaded;
- the Arkivum Automated Data Importer may be used to assist in automating the process of finding data that has not been used and should be archived; and
- there is a developer API for integration with your own applications.

What is the typical transfer time (Mb / min) to and from your data centres?

Transfer times for data to/from the Arkivum service will depend on end-to-end bandwidth between our service and the customer. For guidance, a 100 MB file would take approximately a second to transfer over a 1 gigabit per second connection speed.

How do I know my data has been received correctly?

There is little point putting data into an Archive only to retrieve it many years later and find out that the data archived was not the data you had expected.

The Arkivum Assured Archive uses checksums to provide a unique fingerprint for each file added to the system. The checksums used are industry standard algorithms, which allows you to calculate the fingerprint for the file on your system and compare this to that of the archived file.

If these fingerprints match, then you can be certain that the file in the archive is exactly the same file as the file from your system.

In addition to this, Arkivum provides a simple traffic light system, which shows you clearly when your files have been received at our data centres.

How do I retrieve data from the archive?

The Arkivum Assured Archive service is accessed through an on-site gateway appliance.

This presents the Archive as a windows share or network file system and enables files to be retrieved from the archive in the same way you would copy them from any other drive or share.

In addition to this method, the appliance also provides a web interface, where files can be downloaded and a developer API for integration with your own applications.

Is there an additional cost to retrieve my data?

The cost of transferring data in and out of the Arkivum service is included in the data storage price. Arkivum do not charge 'per GB' transferred in or transferred out. There may be a cost associated with network transfer that is imposed by your network provider, e.g. ISP, depending on how you chose to get connectivity to the Arkivum service, but this is not a charge imposed by Arkivum.

Arkivum does set a fair usage policy on the percentage of data that can be retrieved every month (currently 5%) within the charge for the service. Arkivum is happy to work with customers who need to go beyond this on a temporary or regular basis. For example, on request we can restore data sets to the cache in either our DCs or the customer's appliance so the data is ready for quick access. Bulk exports of data are also possible from our service with physical delivery to a customer site, either as a set of hard drives or data tapes, or as a server ready to be installed locally for rapid transfer of data straight onto the customer's local network. In the case of migration from our service to another provider, the escrow tapes provide a complete copy of data and metadata and are immediately available for transfer of data to a new provider. The cost of the escrow tapes is included in our normal service charge.

How long does it take to get data back?

Data can take up to 5 minutes to start being received by your application, however the times taken will typically be much shorter than this.

Arkivum uses caching at both the appliance and data-centre levels, such that recently added or accessed data can start being retrieved in seconds.

What happens if I want to access the same data several times?

If you're accessing data repeatedly in a short space of time, then the gateway appliance caching will optimise the use of the network link.

The first time an archived file is accessed, the data will be retrieved from the data centre and stored in the local appliance cache. Each additional access of this file will then be serviced from the local appliance, with no need to retrieve data over the network.

How can I do a bulk export?

If you require a large amount of data you can either pre-request this over your network link, or should this take too long, request that data is provided to you in bulk.

This latter option will result in a series of encrypted files being returned to yourself on a tape, or tapes, which you can then retrieve and use at short notice.

How do I know that the returned data is correct?

There is little point putting data into an Archive only to retrieve it many years later and find out that what you have been returned is not the exactly the same as the data you protected.

The Arkivum Assured Archive uses a combination of checksums (mathematical formula to detect changes), multiple copies and active data verification; to ensure your data is returned exactly as it was when placed in the archive.

How much data can I store?

The amount of data you can store is unlimited.

Our Archive service starts at 1 Terabyte (1000 Gigabytes) per annum and scales all the way up to multiple Petabytes (1000 of Terabytes) of data.

Can I modify archived data?

Data cannot be directly modified in the archive. However you can retrieve a file, make changes and check the new file into the archive alongside the original. It is then up to you whether you retain or delete the original file.

Can I delete data?

Deletion of archived content can be managed by a restricted set of users through the administrative interface. This means that files can be removed following a retention period or as required, but cannot be accidentally or intentionally removed during day-to-day usage.

What if I accidentally delete data in the archive? Can you get it back for me?

Data security is an important part of any archive and so if data has been deleted through the administrative interface, then all online copies will have been rendered immediately unreadable.

Due to the unique escrow copy that forms part of the Arkivum service, there will be a short delay before the files are removed from this third offline copy.

If Arkivum is notified promptly of an accidental deletion, before the process of removing data from the escrow copy has been initiated, then it is possible that the encrypted data will be recoverable from the escrow media. To access this data, you will still need to have the master encryption key that was used when the data was archived.

How do I know when it's safe to delete my local copy of the data?

Knowing when your data is safe to remove from your local systems is an essential step in a reliable archive process. At Arkivum we've made this as simple as possible, by providing a simple traffic light system, to show you when your data is safe.

Red	You must not delete your data
Amber	Your file has begun the process of replication
Green	Your file is fully replicated and protected; it is now safe to delete the original.

This simple system leaves no ambiguity, providing a clear way to see when it's safe to remove files from your local storage.

What are your support arrangements (days, times, phone numbers)?

For initial support please contact your reseller where appropriate.

Should this not be possible or you need to speak to Arkivum, then please call our support staff on +44 1249 400 001 or e-mail support@arkivum.com

Support services are provided weekdays, during the hours of 8:30 a.m. to 5:30 pm UK time.

Outside of these times automated alerting systems are in operation, with escalation to a designated analyst.

Integration

What backup tools can you integrate with?

We integrate with a number of backup tools systems and will typically integrate with the archive functionality in any system that can write to a windows share. Currently supported systems include IBM TSM, Enterprise Vault and Marquis Domain Parking.

Please contact us to confirm if we support your preferred backup tools.

How can I identify data that would be good to archive?

Typically 80-90% of the data on an organisation's disk storage has not been accessed in the last year. This type of data is an ideal candidate for archival along with other records that need to be kept for compliance purposes.

The Arkivum Automated Data Importer may be used to assist in automating the process of finding files that have not been accessed recently and should be archived. Please contact us for full details of the Arkivum Automated Data Importer.

What file systems do you support?

The Arkivum service is file system agnostic.

This means that archive can be used from most common operating systems without any additional work.

What content/asset management systems do you support?

We integrate with a number of content management systems and will typically work with any system that can write to a windows share.

Please contact us to confirm if we support your preferred content management system.

Other questions

Do you use de-duplication?

Data stored in the archive is not de-duplicated by Arkivum.

Whilst this may initially seem an odd decision on our part, this helps to increase redundancy of data and hence reliability over the long term. By choosing not to de-duplicate your data we are putting the long term integrity of your data ahead of the ability to save ourselves some storage space.

This doesn't mean that you can't use de-duplication with our service. Should you wish to do so to minimise the amount of data stored, our service can be used as the output target for any one of a number of de-duplication devices.

This does means that, while you will have a smaller stored data set, your retrieved data will have to be processed by the de-duplication device before it can be used and will be subject to the on-going availability of that device.

Do you use compression?

Archived data is not compressed by Arkivum either at a file or media level.

Whilst this may initially seem an odd decision on our part, this helps to increase reliability of your data over the long term. By choosing to not use compression we are putting the long term integrity of your data ahead of the ability to reduce our storage costs.

This doesn't mean that compression can't be used with our service and should you wish to do so the files can be sent to our service via any compression software or hardware.

While you will have a smaller stored data set, your retrieved data will have to be decompressed before it can be used.

Do you provide object storage?

The Arkivum Assured Archive is not block based and will happily store any type of file, be that a simple file or a compound object containing both data and metadata.

While the archive service itself does not function as an object storage daemon (OSD) at this time, it can function as a storage layer under a number of object stores.

Do you support multiple client sites?

Yes, we support multiple client sites.

This is typically through the use of a gateway appliance or virtual appliance at each of the client sites. Once a file has been added to the archive at one site, it will become available to retrieve from the archive at all other sites that are required.

This allows for disaster recovery sites to have access to archived data, without having to maintain a large amount of dedicated archive storage at multiple sites.

What are the firewall requirements?

Firewalls prevent access to and from untrusted sites and services and form an essential part of a company's overall data security policies.

With the Arkivum Assured Archive, only a simple change is required to allow our service to operate through an existing corporate firewall.

Just allow access from your network to our data centres on UDP port 1194 to allow the gateway appliance to create a secure connection to our secure storage locations.

Appendix A – Theoretical case study to illustrate the differences between direct loss and indirect or consequential loss

The following theoretical case study, of an insurance intermediary organisation, illustrates the difference between direct loss, and indirect or consequential loss. This Organisation has a regulatory obligation to keep recordings of its telephone calls with clients and has decided to implement an Arkivum data archive service.

Through a chain of unfortunate events the organisation finds itself being sued by one of its clients for negligence. During the Court hearing the organisation is ordered to provide all records of correspondence, including telephone calls, to be used as evidence.

Regrettably, when the organisation attempts to retrieve the data from Arkivum's archive a problem occurs and all three copies of the recordings are discovered to be corrupt.

The organisation is therefore unable to comply with the Court's order. It is also subject to a regulatory fine for its failure to ensure that telephone calls with its clients are recorded and archived appropriately.

The regulatory fine imposed on the organisation is a direct consequence of the failure of Arkivum's service, therefore the organisation will be able to claim against Arkivum for the loss it has suffered i.e. the amount of the fine, subject to the cap on Arkivum's liability.

Notwithstanding the organisation's inability to produce the recordings, the Court duly considers the evidence before it and its judgment goes against the organisation, awarding damages to the insurance intermediary's client. It is possible that the missing recordings might have provided the organisation with a complete or partial defence to the claims made against them. To the extent that it can be established that this is the case, the organisation will be entitled to claim against Arkivum for the damages and costs that it must pay to its client. This is a direct loss for which Arkivum is responsible as stated above.

The organisation finds that the time its managers have had to spend in conducting its defence has been increased by its inability to produce the recordings and subsequently seeks to obtain compensation for its reduced revenue resulting from the loss of business opportunities the managers would otherwise have been able to pursue. This, however, will not be a recoverable loss, as it is both an example of Excluded Loss, and an example of indirect or consequential loss.