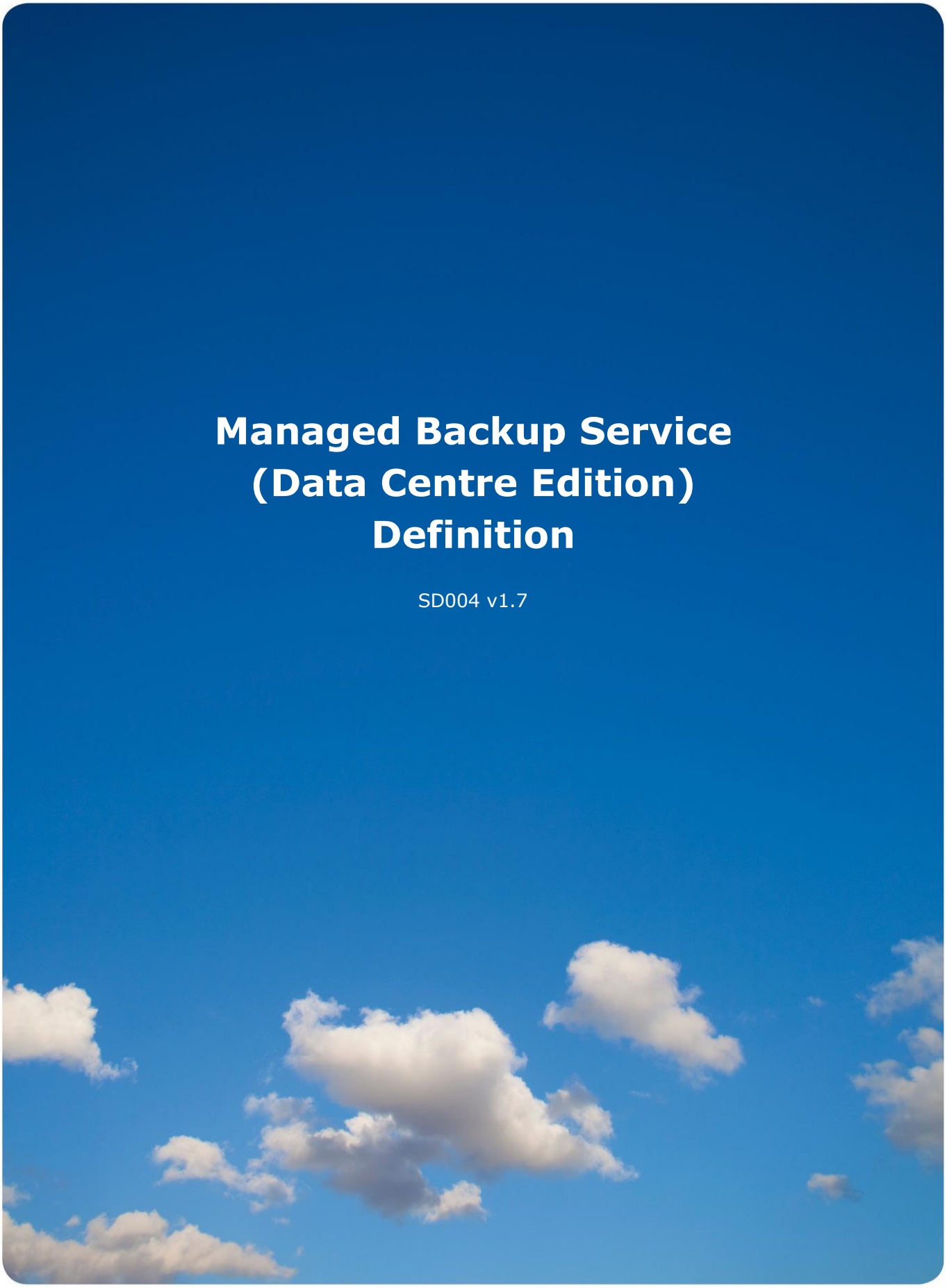
inTechnology



Managed Backup Service (Data Centre Edition) Definition

SD004 v1.7

Managed Backup Service (Data Centre Edition) Service Definition

Service Overview

The InTechnology Managed Backup Service (Data Centre Edition) service provides a managed backup and archive service for customer servers located at their centralised / data centre premises. The customer's servers are connected over a high bandwidth network connection to a backup server and dedicated disk or tape storage capacity within an InTechnology data centre.

The Managed Backup Service consists of backup clients and application agents installed on the customer's servers that require backup or archive services. These clients and agents provide two complementary but separate functions: backup and archiving of file system and application data.

The backup function provides regular backups of critical business data on the customer's servers. Regular backups, typically run daily, should be performed for business continuity purposes. File system backups are performed on an incremental basis. The first backup taken is a full backup and all subsequent backups are incremental only. This reduces the backup window required to backup customer servers and the overall quantity of backup data to be stored on disk or tape. Schedules can be configured on the backup server to automatically backup clients as required.

Supported applications are backed up independently of file system backups and use application specific agents. Application agents typically perform a cycle of full and incremental backups. Schedules can be configured on the backup server to automatically backup agents as required.

The archive function complements the backup function by providing archiving, for file system data held on the customer's servers. An archive operation is a single "point-in-time" copy of file system data on the customer's server that is retained for a specified period of time. Typical uses of archiving include year-end copies of important data required for legislative purposes and near-line storage of rich text data such as voice or video images.

The backup client performs the archive and transmits the archive data to the backup server. Optionally, the archived data can optionally be automatically deleted from the server after a successful archive operation.

Backup and archive data is stored in a network attached disk array or tape library. By default all backup and archive data for a customer server is located on separate disk drives or tapes. There is no sharing of disk drives or tapes between customers.

Once stored on disk or tape backup and/or archive data can be replicated to additional disk or tape volumes. This feature provides additional protection against data corruption or hardware errors. The default is a single of copy of data is stored.

The Managed Backup Service is monitored and managed to an agreed SLA by InTechnology's 24x7 customer Support and consultancy staff. The service includes extensive remote and on-site consultancy support to ensure that the service is implemented and maintained to the highest standard to meet our customers' backup, recovery and archiving requirements.

Service Definition

The Managed Backup Service (Data Centre Edition) delivers a fully automated and managed network backup and archiving service for customer servers located at the customer's central premises / data centre.

The service at the customer location consists of backup clients and agents installed on the customer servers to be backed up. Within the InTechnology data centre the service comprises of a backup server and dedicated disk or tape capacity.

Customer Network Connection

The Managed Backup Service (Data Centre Edition) requires a dedicated InTechnology provided network connection, including a router installed at the customer premises. The router manages the network connection between the customer LAN and the InTechnology data centre. The router is connected to the customer's LAN via a 10/100 Ethernet connection. TCP/IP is the only supported network protocol for the router network interface. The customer is responsible for providing an appropriate static IP address for this interface, normally the first address in the range supplied to InTechnology.

The router is connected to the InTechnology secure private network through a dedicated LAN extension circuit. This enables the backup clients and agents on the customer servers to transfer the backup data to the backup server in the InTechnology data centre. The leased line circuit is fully managed and is delivered from the nearest Point of Presence (POP) on the InTechnology network. The appropriate bandwidth capacity is determined by the individual customer's requirement. Typically, the circuit capacity is specified to accommodate current requirements, speed of restore and anticipated future growth in data volumes. The leased line circuit is arranged and managed by InTechnology and made available exclusively for each customer. A minimum bandwidth capacity of 100mb/s will be installed.

Backup Clients and Agents

Backup clients and agents installed on the customer servers perform the backup, restore and archiving functions. The backup client or agent transmits the backup and archive data to the backup server. There are two types of agents: file system clients and application agents.

File system agents can backup and archive all data stored within file systems on the server platforms supported by the Managed Backup Service. Schedules can be configured on the backup server to automatically backup clients as required.

Applications supported by the Managed Backup Service can be backed up independently of file system backups by using application specific agents. Application agents typically perform a cycle of full and incremental backups. Schedules can be configured on the backup server to automatically backup applications as required

Data Encryption

File system backup and archive data can be selectively encrypted; either at an individual file, directory or at a file system level; using standard DES 56-bit encryption algorithms. Data is automatically encrypted before transmission to the InTechnology data centre and is stored by the backup server in encrypted form. Data is automatically decrypted during customer restore operations. Encryption is an optional service and is controlled by client configuration options for the Windows, AIX, Solaris, HP-UX, NetWare, SGI, Linux, NUMA-Q and TRU64 file system backup clients.

The customer is responsible for entering individual encryption keys for each customer server during installation of the file system backup clients. Once this configuration is complete the encryption key is stored securely on the customer server and is used automatically during subsequent backup and restores. If the stored encryption key is destroyed on the customer server, e.g. during a server disaster recovery, or data is being restored to a different customer server, the customer will be prompted during

the restore operation to enter the appropriate encryption key. Failure to enter the correct key in these scenarios will prevent data restoration.

It is the customer's sole responsibility to maintain a satisfactory record of their encryption keys. Failure to do so will result in encrypted backup and archive data becoming inaccessible in the event of a customer server or site disaster. InTechnology has no record of encryption keys used by the customer and cannot recover customer data in the event of the customer losing their encryption keys.

Note: there is currently no encryption support for application agents.

InTechnology Supported File System Platforms

The Managed Backup Service is based on an IBM Tivoli Storage Manager (TSM) v5.5. server platform and supports the following operating systems. InTechnology will make all endeavours to support future versions of the operating systems below. Other platforms might be subject to a surcharge.

Operating Systems
Windows
Solaris
Linux
Novell NetWare

Customer Supported Platforms

The following operating systems and databases are not supported by InTechnology, but are can be backed by the customer.

Operating Systems
IBM AIX
HP-UX
Linux
Macintosh

Support for additional server operating systems not listed may be possible and are subject to the appropriate backup clients being available. An additional service charge will apply for installation of these clients.

The file system backup clients for the above platforms are installed and configured by InTechnology consultants as part of the MBS service implementation. Optional pre- and post-backup scripts can be defined during the service set up to stop and start applications or to perform other server tasks. Creation and maintenance of pre and post-backup scripts is the responsibility of the customer.

Backup Client User Interface

The file system backup client contains all components required to perform backups, either scheduled or manual, restore and archiving operations. The client scheduler for scheduled backups and archives is typically installed as an automatic service or process and requires no user intervention once configured.

The clients provide three user interfaces for performing ad-hoc backups, archives and restore operations: a command line interface, a GUI interface and a Java based Web browser interface. The command line

and GUI interfaces can be used locally on the server or remotely over a network connection. Typical methods of using the command line or GUI interfaces remotely are Telnet, X Windows, Windows Terminal services or equivalent. The Web browser interface can be used either locally or remotely via a TCP/IP network connection. As part of the service implementation, training on use of the backup clients will be provided to appropriate customer personnel.

InTechnology Supported Application Platforms

The Managed Backup Service supports the following applications and databases:

Application
MS Exchange
MS SQL Server
Oracle
VMware

The application agents for the supported applications are installed as part of the service implementation. InTechnology consultants perform installation and configuration of the application agents, in conjunction with the appropriate customer database or application administrator.

The supported application agents only backup the appropriate application data. In addition to the application agent the appropriate file system backup client must also be installed and configured to backup the remaining file system data on the customer server. There is no online archiving support for applications. Application data to be archived must be extracted using techniques such as database dumps and then archived.

Customer Supported Application Platforms

The following applications and databases are not supported by InTechnology, but are can be backed by the customer:

Application
Informix
Lotus Domino
SAP R/3
WebSphere

Application Agent User Interface

The application agents have user interfaces appropriate to the application environment. For Windows based applications such as Exchange, SQL and Lotus Notes, GUI and command line interfaces are provided.

For other applications, the agent user interface is typically integrated into an application related administrative interface. Examples of these are Oracle's Recovery Manager (RMAN) utility and the SAP R/3 SAPDBA database utility. As part of the service implementation, training on use of the backup agents will be provided to appropriate customer personnel.

Data Restoration

It is the customers' responsibility to perform restoration of data. The appropriate user interface can be invoked to restore single files, multiple files, complete file systems or applications as appropriate.

InTechnology personnel have no access to the backup clients and agents on the customer servers and cannot perform restore operations.

To assist the customer in developing tested restore procedures, InTechnology consultants will deliver customer specific "best practices" for recovery of the appropriate customer server and application during the service implementation. The Managed Backup Service is a network-based backup, restore and archiving service. If the customer server has been rendered inoperable to an extent where the backup client or application agent cannot run, then this must be rectified prior to performing the restore operation.

Backup Server

The Managed Backup Service utilises one or more customer backup server in an InTechnology data centre. The backup server is connected to a disk storage array or tape library used for backup and archive data.

Disk storage

The disk storage is used for the backup server database and might also be used for backup and archive data. If the customer opts for disk storage a single copy of all backup and archive data is stored on disk volumes by default throughout its retention period. For enhanced availability data can be automatically replicated to secondary disk volume. This replication can be applied selectively to some or all of the backup and archive data. Replication can be performed to a second disk storage that is located in a second and geographically diverse InTechnology data centre.

Tape storage

If the customer opts for tape storage a single copy of all backup and archive data is stored on tapes by default throughout its retention period. For enhanced availability data can be automatically replicated to secondary tape storage pool. This replication can be applied selectively to some or all of the backup and archive data.

Backup Policies

Backup data from backup clients and application agents is managed based on policies defined on the backup server. These management policies define the number of backup generations, expiration of deleted files and handling of open files during backups.

The Managed Backup Service provides separate backup policies for file system data and applications. There is a default set of policies for file system data that will be further refined as appropriate during the service implementation. Policies for application data are bespoke for the application and will be defined in conjunction with the customer during the service implementation. Backup and archive policies and schedules are defined and stored centrally in the backup server database.

File System Backup Policies

The Managed Backup Service does not emulate legacy "tape rotation" based backup products where cycles of daily, weekly and monthly tape cartridges are required. With this method a weekly backup must be performed and then daily incremental backups. This causes a larger requirement for storage capacity.

File system backups are performed on an incremental only backup basis. The first incremental backup is a full backup and all subsequent backups only backup the data changed since the previous backup.

For example, if a 20GB file system is backed up the first backup will result in approximately 10 GB of backup data (assuming an average compression ratio of 2:1). If the next day 10% of the data has changed then an additional 1GB of backup data is stored (2GB compressed to 1GB). This process carries on every day thereafter. No further full backups are required. The quantity of data stored is managed by

policies that determine the number of backup versions held for individual files. The more versions held, the more data would be stored.

The number of backup versions also determines how far back a restore operation can be performed. A default restore will restore the most current version of every file resulting in a recovered file system to the exact state it was in at the time of the last backup. Alternatively a restore date can be specified. In this case the most recent backup for every file prior to the specified date will be restored. The greater the number of versions, the further back the restore operation can be performed.

The default backup policy for file system data is:

- Four generations of backups will be stored for files that have been modified. Files that are never modified will only be backed up once on the initial backup.
- For files that have been deleted on the customers' server the most recent backup generation will be maintained for 90 days. After 90 days the final backup will be deleted.
- For files open and locked by other applications up to 4 attempts will be made to back up the file. If after the fourth attempt the file cannot be backed up, it will be bypassed by that backup session.
- By default, all files on all locally attached file systems are backed up. Files can be excluded from backup during the initial service configuration.

For example, two backup policies could be created for file system data that store 7 or 14 generations of file backups. These backup policies will enable point-in-time restoration up to 14 days prior to the last backup. However, they will result in more stored backup data. These optional backup policies can be selected during the backup agent installation and configuration. These backup policies can also be further developed during the service implementation.

Application Backup Policies

The backup policy for applications on customer servers is dependent on the specific application. Typically this will include two weekly full backups and daily incremental backups. In this scenario two weeks’ worth of backups are retained. The precise management policies will be determined as part of the implementation planning.

Archive Policies

Archive policies are separate from backup policies and define the retention period for archived file system data. The archive retention period can be defined to a granularity of one day – for example, a retention period of 365 is one year. The default archive retention period is 3 years, after this time the data is automatically expired and deleted from the archive store. Alternate retention times can be defined to meet specific business requirements. If required, an indefinite retention period can be defined and the archived data will be retained forever. Multiple archive policies can be defined to address differing business requirements.

Backup and Archive Schedules

Backup operations can be scheduled for automatic operation. Schedules are defined, stored and managed from the backup server in conjunction with the appropriate customer personnel.

The default schedule is for a backup that commences between 20:00 and 24:00, seven days a week. The actual start time of the backup will vary due to workload and network resource constraints. Additional backup schedules as appropriate will be defined during the service implementation.

Archive operations can also be scheduled for automatic operation. However, because of the ad-hoc nature of archive operations no default archive operations are defined. Archive schedule requirements will be defined in conjunction with the customer during the service implementation.

Disaster Recovery

In the event of an event requiring a large data restore, e.g. loss of a server, the normal method of restore is over the network from the backup server in the InTechnology data centre. However, in the event of a customer site disaster the leased line connection would not be serviceable. To accommodate this scenario the Managed Backup Service incorporates provision for customer site disaster recovery where the leased line connection is unavailable.

As part of the project definition workshop the InTechnology consultant will work with the customer personnel to identify their disaster recovery requirements. This will involve designating the servers with a high, medium or low disaster recovery classification.

In the event of a customer site disaster InTechnology will ship a portable backup server and disk array or tape library to the customer's nominated disaster recovery location. This portable service will contain the backup data for the high priority customer servers and copies of the appropriate backup clients and agents for the replacement customer servers. An InTechnology consultant will travel to the customer disaster recovery location to assist with the setup of the service and recovery of data.

Following the recovery of the high priority server(s) backup data for the medium and low will be shipped to site on agreement with the customer. No archive data will be provided as part of this disaster recovery service.

DR Testing

Disaster recovery tests can be scheduled. In this scenario the production Managed Backup Service will be maintained and scheduled backups and archives can continue at the primary customer location. Disaster recovery testing is an additional chargeable service option.

Service Implementation & Support

MBS is a managed service that includes four consultancy modules to provide the Project Definition Workshop (PDW), service implementation, service support and provide ongoing project management for the solution. Following successful completion of the first two elements, the InTechnology consultant and the customer will sign off the MBS as being fully implemented.

Project Definition Workshop (PDW)

The implementation planning consultancy service provides the customer with a cost-effective way of ensuring a well-designed backup solution for more complex configurations and a smooth and efficient implementation. This service is designed for any customers who have backup requirements over and above basic file systems such as database applications. It encompasses:

- A review of the customers backup/restore requirements
- A check that the technical environment is ready for the implementation
- A design for the service implementation to meet the customer's backup/restore requirements
- Capacity requirements for the leased line circuit, backup server(s) and disk / tape storage
- A schedule for the implementation of the service environment
- An agreed set of acceptance criteria

In order to ensure that maximum benefit can be gained from the work, the consultant(s) will need to work closely with customer staff with the appropriate system knowledge and be provided with suitable access to systems if required.

A schedule for completion of the tasks outlined below will be agreed prior to commencing the work.

Project Tasks

1. Prior to the start of the project the InTechnology consultant(s) will contact the customer to agree schedule for the customer meeting and information that the customer needs to provide

2. As agreed with the customer the InTechnology consultant(s) will meet with the relevant customer technical staff and inspect the technical environment.

3. Development of the implementation plan.

Project Deliverables

The result will be an implementation plan that will cover the following:

- Configuration requirements for backup and application agents.
- Details of any server configuration changes, server code patch levels, etc.
- Network topology design for the customer servers to connect to the router
- Backup policy classes and schedules
- Disaster recovery requirements
- A schedule for the implementation
- Documentation of the solution

The implementation plan will be available within 10 working days of the completion of the PDW.

Service Implementation

During installation of the Managed Backup Service, InTechnology consultants will provision and install the hardware and software components. There are a number of elements to the installation:

1. Backup server installation

2. Installation and initial configuration of the router on the customer site

3. customer training

4. Installation and configuration of the clients and agents on the customer's servers

5. Service hand-over

Backup server Installation

The backup server(s) will be implemented following the order of the leased line circuit but prior to the final implementation of the leased line. InTechnology will build, configure and test the backup server to an initial configuration based on the specification agreed with the customer during the implementation-planning phase.

Router Installation

InTechnology will arrange a convenient time just prior to the final delivery of the leased line circuit to install and configure the router. Following installation of the router and successful testing of the LAN extension circuit, the backup and application agents will be installed, configured and tested. Appropriate

customer personnel will be required to work with the InTechnology consultants during this phase to ensure an agreed implementation.

Customer Training

Before or during the provision of the Managed Backup Service, the appropriate customer personnel will be trained how to use the backup and application agents to perform backup, restore and archive operations, and use of the web reporting interface. This training is mandatory. In most case this training is going to be delivered onsite, as part of the service installation. Alternatively InTechnology may decide to provide this training at one of InTechnology's offices.

Backup Client Implementation

During the service implementation InTechnology consultants will work with the appropriate customer personnel to install and customise the backup agents as defined in the service implementation plan.

The backup clients will be implemented based on the InTechnology "best practice" consultancy modules. These best practice consultancy modules, document InTechnology's extensive practical experience in the installation, performance tuning and recovery procedures for the backup agents.

Application Agent Implementation

Application agents are used to perform online backups of the supported applications. These are implemented to backup the database using the applications own API's. The vendor whose application is being backed (e.g. Microsoft or Oracle) produces these and thus the agents are certified to backup these applications. The agents are used to backup databases, online, offline, full or partially.

The customer must determine which type of backup best meets their business needs. This is discussed in the PDW. The Database Administrator must be available for the implementation of these modules as it is essentially they who are responsible for these applications. The main thing to remember is that the backup server is just a storage repository for these backups. The application agent is responsible for taking the data and passing that on to the backup server.

The InTechnology consultant will work with the DBA to ensure that the backup server is set up to store the application data to meet business needs. The InTechnology consultant will also set up schedules to automate the backup of the databases. The DBA must ensure these schedules complete successfully and the application is in the correct state for the backup action, i.e. online, offline or quiesced.

Implementation Testing

Subsequent to the installation phases detailed above an InTechnology consultant will perform and implementation test to demonstrate the working service in accordance with the acceptance criteria defined in the PDW.

Backups and restores will be tested between the customer site and InTechnology's data centre. It is important for the customer IT personnel to be present during this phase as it is an integral part of the education process.

Once testing has been completed to the satisfaction of both parties, the service will be deemed operational and handed over to the InTechnology Support Team for ongoing management. At this point charging will then commence.

To ensure a smooth transition from implementation to live service, it is important that the InTechnology Support Team is involved in the latter stages of the installation. Working in conjunction with the InTechnology consultant, a support specialist will assist with the final testing and documentation phase, to ensure an effective hand-over.

It also allows the InTechnology support representative to introduce himself or herself to the customer and present a welcome pack, which explains support procedures such as call logging, escalations, etc.

Post Implementation Review

One month after the installation an InTechnology customer implementation engineer will contact the customer to arrange a post installation review. The purpose of the review will be to address any issues the customer may have and to ensure that the Managed Backup Service is providing the protection to the customer's data.

Service Support

InTechnology will manage the Managed Backup Service to an agreed SLA. As part of the SLA, InTechnology will provide remote monitoring from an InTechnology data centre and onsite support to an agreed service level.

Infrastructure Support, Monitoring & Management

The Managed Backup Service is supported by a comprehensive support, monitoring & management package that enables 24-hour monitoring of all hardware, software and network elements including:

- Event reporting and analysis
- Response to systems alerts
- customer notification of system alert
- Collection of data and management information
- Backup server hardware or software errors
- Disk hardware errors
- Connectivity errors
- Backup failure

Errors affecting the availability of the service are escalated to InTechnology's 24x7 service support staff and/or service support groups for immediate action. Errors or events relevant to the customer server backup or restore functions are notified to the customer via the web reporting interface.

Remote Technical Support

The Managed Backup Service includes remote telephone support from the InTechnology service support centre. Remote support is provided to advise on general enquiries such as backup agent operation questions, configuration changes or diagnosis and resolution of problems as required.

Service Level Agreement

Objectives

This section details the agreed target levels of performance of the Managed Backup Service provided by InTechnology to the customer. It is envisaged to keep this document updated on regular intervals if and when changes are required.

Introduction

1. Detail of the level of services to be provided by InTechnology for the Managed Backup Service in terms of availability and response time.

2. Detail of the specific responsibilities for both InTechnology and the customer to ensure that the Managed Backup Service is properly commissioned.

3. Definition of the mechanism reviewing InTechnology's performance in providing the Managed Backup Service.

4. Definition of what will happen in the event that a problem occurs.

5. Detail of those circumstances under which the service will be deemed to be outside of the Service Level Agreement.

Unless stated, InTechnology will report all measures monthly to the customer.

InTechnology Responsibilities and Obligations

InTechnology will provide an automated mechanism whereby the customer will be able to backup data from all designated servers as defined in the output produced from Project Definition Workshop. Subject to the conditions outlined in this document InTechnology will undertake that the service delivered to the customer will function as specified.

Installation and Configuration

An authorised InTechnology representative will deliver the specified services to the designated location on a pre-arranged installation date, or dates, to be agreed on signing of this Agreement. All defined products and services will be installed, commissioned, and tested to ensure that the equipment and software is functionally operational. An InTechnology authorised representative will demonstrate to a nominated customer representative that the service is capable of backing up data from the customer's servers and restoring data.

At this point, the InTechnology authorised representative will hand over the Managed Backup Service to the customer and notify the InTechnology customer support team that the service is live and fully commissioned. The InTechnology authorised representative will present the nominated authorised customer representative with a service signoff document.

Training

InTechnology will provide training for the nominated customer representative as defined in the Service Definition. As a minimum, the authorised customer representative will be trained to backup and restore data from the Managed Backup Service Server. Additional training can be purchased from InTechnology.

Support Process

InTechnology will provide the customer with access to a manned 7 days, 24 hours customer support team. Calls will be handled strictly in accordance with the escalation process outlined in the customer Service Plan section of this document with priority being given to the most severe.

Backup and Restore of customer Data

Within the terms of this SLA, InTechnology will be responsible for ensuring that the Managed Backup Service and all associated components will be available to backup customer data from defined customer servers (as per PDW). InTechnology will be responsible for ensuring that the Managed Backup Service and all associated components will be available to restore customer data that has been previously backed up from defined customer servers.

Reports

InTechnology will be responsible for defining and delivering the reports pertaining to the availability of the Managed Backup Service and response/fix time of the Support team.

Customer Responsibilities and Obligations

Although the Managed Backup Service is a managed service proposition and InTechnology will be responsible for the availability and support of the service components, the day-to-day operation of the Managed Backup Service will, in part, depend on certain key processes and related equipment which are wholly under the customer's control. The customer will also be responsible for the provision, installation, management and support of any customer internal network connectivity required to deliver this service.

Installation and Configuration

The customer will make available a nominated and appropriately qualified representative to work with the InTechnology representative during the installation of all the necessary services components, as defined in the Agreement. The nominated customer representative will confirm that the backup functionality and subsequent restore capabilities of the service has been demonstrated to his/her satisfaction. The nominated customer representative will then accept delivery of the Managed Backup Service as a fully commissioned service. The nominated customer representative will sign the service signoff document and present this to the InTechnology authorised representative.

IMPORTANT: if encryption is implemented as part of the service offering, then the customer is solely responsible for storing their encryption keys in a secure location. Loss of the keys by the customer will prevent recovery of the customer's backup data.

Training

The customer will be responsible for nominating a representative to undertake the InTechnology Managed Backup Service training as defined in the service definition. As a minimum, the customer will ensure that at least two nominated people are capable of backing up and restoring data using the Managed Backup Service clients/agents and escalating a problem using the procedures outlined in the Support Process section of this document.

Support Process

The customer nominated representative will be responsible for promptly reporting any problems directly to the InTechnology customer support team in accordance with the escalation procedures outlined in the customer Service Plan section of this document.

Customer Backup and Restore of Data

The customer will be responsible for defining appropriate server backups and advising InTechnology of the required schedules. The Managed Backup Service cannot guarantee to successfully backup all open files. The open files that fail to backup are reported to the customer by Managed Backup Service. The customer will be responsible for reviewing such occurrences and modifying their backups as appropriate. The Managed Backup Service only reads data for backup and cannot verify logical data integrity. It therefore remains the customer's responsibility to ensure that data integrity, including virus checking, is maintained. The customer will be responsible for performing all data restore operations.

Reports

The trained customer representative will be responsible for reviewing and acting upon the reports and logs provided by the Managed Backup Service.

Availability

This is the measurement of whether the Managed Backup Service is available for backup and restore (this does not take into account the Service Connection).

MBS Availability	Equivalent downtime per month (24 x 7 x 365)
99.0%	7 hours 26 minutes

Total Service Outage

When a platform or system upgrade is planned that will result in a total system outage affecting all customers, InTechnology will endeavour to give 7 days prior notice to allow customers time to limit any impact on their own operations.

Service Credits

The following service credits will apply based on the criteria detailed in the Managed Backup Service availability section above. In the event that the Managed Backup Service falls outside of the SLA, i.e. the downtime on the Managed Backup Service exceeds a cumulative total of 7 hours and 18 minutes (99.0% availability) in any one month, then a service credit shall apply based upon a percentage of the maximum service credit per instance as calculated below.

Maximum service credit per instance =Total monthly Managed Backup Service charge

The table below details the applicable service credits based on the number of instances in any one month.

Total number of instances of the Service falling outside of SLA in any one month	Percentage of maximum service Credit paid per instance
1	5%
2	10%
3	20%
4	30%
5	40%
6	50%
7	60%
8	70%

9	80%
10	90%
11+	100% (Maximum)
Where any one instance exceeds the SLA and the Managed Backup Service is unavailable for operation (i.e. the customer is unable to perform a backup or restore) for longer than 24 hours then the service credit for that particular client instance will be:	100% (Maximum)
Important: Regardless of the total number of client instances the total service credit paid in any one month will not exceed the total monthly service charges for the month.	

Managed Backup Service (Data Centre Edition) Charges

Installation & Monthly Charges

The following table details the charges associated with installation of the Managed Backup Service as well as the monthly service charges. Please note a requested change in configuration may require some or all of the components of the Service to be changed and thus result in additional charges.

Service Element
Service Implementation

Charging Model

Default Service Elements
Minimum disk / tape capacity
Additional disk / tape capacity
1 x TSM backup server

Software Management Charge

Client & Agent Type	Description
TSM Extended Edition Client License (per desktop/laptop)	Backup agent for desktops and laptops
TSM Extended Edition Processor License	The TSM Extended Edition covers all file and print servers and can be deployed for the following operating systems: AIX 5L V5, Apple Macintosh, Compaq Tru64, HP-UX 11.x, IRIX (Silicon Graphics), Linux for System i, Linux for System p, Linux for System x 86Series, Linux for System z, Novell Netware, OS/400 V4.x, Red Hat Linux, SUSE Linux, Solaris (Sun Microsystems), Windows 2000, Windows NT, Windows Server 2003, Windows XP
TSM for Mail	Backup Agent for Exchange and Lotus Domino.
TSM for Databases	Backup agent for SQL, Oracle, DB2 and Informix.
TSM for Application Servers	Backup agent for other applications
TSM for ERP	Backup agent for ERP servers.
TSM for SAN	Backup agent for SANs.

Notes on Charging

- All server and application license are based on dual processors per server. For each additional processor the software management charge will increase by 50% for that particular license. If only a single processor is used the cost is halved.

Monthly Charges

- The Monthly Storage Charge is a fixed charge based on the contracted configuration of the Managed Backup Service in the InTechnology Data Centre in each month.

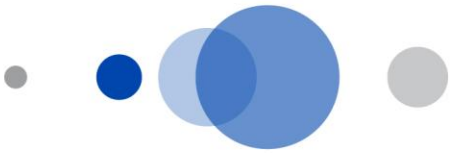
- The Monthly Software Management Charge reflects the configuration complexity and number of customer servers and applications to be managed by the Managed Backup Service. The Monthly Software Management Charge (SMC) also covers client and agent updates to ensure ongoing compatibility with the customer applications and operating systems. As additional servers and applications are added or removed, the Software Management Charge will be amended to reflect this.

Generic Notes on Charging

- The service activation charge will be invoiced upon signing the Service Agreement.
- Service activation charges cover the installation of Services during normal working hours (09:00 – 17:00, Monday - Friday). Installations required outside of these hours will be charged at an hourly rate. Installations requested by the customer to be undertaken outside of normal working hours should be agreed in advance between InTechnology and the customer and must be accompanied by a customer specific purchase order or an email of intent.
- The Monthly Charges will be billed monthly in arrears. The billing period starts as soon as the Service has been activated and made available for use
- Important: The initial monthly charge has been based on information provided by the customer, in particular an estimate of the volume of data to be replicated, backed up and / or archived.
- It is recommended that the customer maintains their existing backup solution until Phase 2 installation (as detailed within the MBS Service Definition) is complete and signed off
- A man-day for consultancy services is defined as 09:00-17:00. Expenses are included in the charge unless otherwise agreed.
- The sizing of the all service components has been based on information provided by your own employees. Any subsequent configuration changes required for any of the service components as a result of increased workload, data volumes or managed servers will result in an amended Monthly Charge.
- The initial software management charges (where appropriate) is based on information provided by your own employees. InTechnology will provide appropriate software licenses to meet this requirement. Addition or removal of customer servers and / or increasing the number of licenses required will result in an amended monthly license charge.

Service Exclusions

- Rebuild of customer hardware or operating system environment.
- Support for operating systems other than replication, backup & recovery and /or archiving issues related to the operating system.
- Support for customer's network infrastructure.
- Support for customer's application software.



InTechnology designs and supports the best IP solutions for business with a range of applications seamlessly integrating clients' communications needs through the delivery of secure voice, data and mobile solutions.

InTechnology employs 200 people and has data centres in Harrogate, London and Reading.

Head Office

Central House
Beckwith Knowle
Harrogate
HG3 1UG
Tel: 01423 850 000

London Office

17 St Helens Place
Bishopsgate
London
EC3A 6DG
Tel: 0203 040 5000

Reading Office

Commensus House
3 – 5 Worton Drive
Reading
RG2 0TG
Tel: 0870 777 7778

Enquiries: 0800 528 2522
www.intechnology.co.uk

inTechnology