VDC Operations Annex – Managed

Additional Terms for VDC Managed

CONTENTS

1 SOW

For each Solution, Interoute will provide an SOW. The SOW is established based upon the Customer's requirements. Interoute is not responsible for ensuring that the SOW is fit for the particular purpose of the Customer. The Customer agrees that the SOW is fit for the particular purpose of the Customer.

2 ON-BOARDING

Interoute will be responsible for the deployment and configuration of the Service, according to the SOW.

3 SERVICE OPERATION

Interoute will be responsible for the operation of the Service, as set out within this annex.

3.1 CUSTOMER ACCESS

Interoute will provide the Customer with "administrator" or "root" level access to the Operating System, in order for the Customer to manage elements of the system other than the Operating System such as Customer Serviced Software, applications and data. The Customer agrees not to modify any Interoute Serviced Software configuration without prior consent from Interoute.

3.2 SOFTWARE LICENSING

Interoute will procure and maintain the relevant licensing for:

a. Microsoft Windows Server,

b. licenses required to deliver the features of the VDC Managed Service,

c. other licenses specified in the SOW as 'provided by Interoute'.

3.3 ANTI-VIRUS UPDATES:

For servers running Microsoft Windows Server, the anti-virus update process will perform signature updates every 4 hours (if new updates are available).

3.4 PATCH MANAGEMENT:

The Patch Management Process will take place once per week.

3.5 SERVICE MONITORING:

Interoute will setup Monitor(s) and configure default Monitor Threshold(s). Where a Monitor Alert is triggered by the breach of a Monitor Threshold, Interoute will raise a support Ticket and notify the Monitor Contact.

3.6 SERVER BACKUPS & DATA SNAPSHOTS

3.6.1 Backup Capability & Granularity

Interoute will provide backup capability for Customer data. This will include Operating System data and configuration. Backups are performed online at file system level only and do not provide support for open file application data. Specifically, transactional files used by various applications such as database volumes or hibernation memory can be backed up, but are required to be in a "dumped" and "closed" state before the backup operation starts, otherwise the files may be in a corrupt state once they are restored. Interoute does not accept responsibility for the corruption of such files or for any damage caused to the VDC Managed Service by such corrupt files.

Interoute reserves the right to exclude from backup at its sole discretion files that may affect the ability to recover from a failure.

3.6.2 Backups Schedule and Data Retention

Interoute will perform scheduled, daily incremental backups for six sequential days followed by weekly full backups every seventh day as determined by Interoute. The backup images for the full backups are retained for a 28-day period and for the incremental backups for a 14-day period after which time they shall be disposed of or overwritten.

3.6.3 Data Snapshots

Snapshots that are implemented as part of the Solution or are included with a deployed VDC storage Service Component are subject to the technical capabilities of the Service Component as defined in the VDC technical datasheet (subject to change by Interoute from time to time and available upon Customer's request).

4 INCIDENT MANAGEMENT

Further to the provisions in Schedules 1 and 2N, Interoute will provide incident management for the elements of the VDC Managed Service and the Service Levels defined within the SLA Annex. In addition, Interoute will provide data restore actions as follows:

4.1 DATA RESTORE

Any data restore necessary due to an Incident, not attributable to Customer, will be conducted at Customer's request on a 24x7 basis.

If Interoute responds to and works on a reported Incident and it is subsequently found to be attributable to the Customer, then Interoute reserves the right to apply Professional Service Charges in respect of the time spent resolving the Incident.

It is the Customer's responsibility to recover all applications to their desired state after a data restore. Interoute is not responsible for loss or corruption of data caused by incompatibility of the Customer Software and Interoute's backup software.

4.1.1 Backup restore

The restore of a backup will only restore the files or folders specified by the Customer. Restoration will only be to the original or alternate VDC location as specified in the SOW.

4.1.2 Snapshot Restore

The restore of a snapshot will replace all the data of the storage volume with the data of the specified snapshot.

5 CHANGE MANAGEMENT

Customer is entitled to submit change requests to Interoute at any time. Where a request is made to Interoute to implement a change to the Service, Interoute will consider such changes. Where changes are likely to result in additional work beyond the standard management of the Solution as set out within this annex and the SOW, Interoute will advise the Customer of any additional charges that Interoute may require in order to complete the work, applying Professional Service Charges or such other charges as are agreed at the time between the Parties.

5.1 CHANGES TO VIRTUAL MACHINES & STORAGE VOLUMES

The Customer can request changes to the Virtual Machines virtual hardware specification and storage volume sizes by raising a Ticket using the My Services portal.

5.2 CHANGES TO LOAD BALANCERS

The Customer can request changes to a load balancer policy by raising a Ticket using the My Services portal. The standard changes are:

a. Configuring virtual server IP addresses (VIPs) for load balancing.

b. Adding, deleting or changing member IP addresses of vIPs.

5.3 CHANGE CONTROL

Interoute's responsibilities for change control include tracking proposed and completed changes to systems and Services managed by Interoute, and informing Customer of any proposed changes that may impact on Service performance/availability.

6 CUSTOMER RESPONSIBILITIES

Further to the provisions in Schedules 1 and 2N, the Customer agrees not to directly access Interoute Serviced Software or modify any configuration on the Solution without prior written consent from Interoute.

In addition to the responsibilities laid out within Schedule 2N the Customer undertakes that it shall:

a. ensure any reboots or stopping of Interoute monitored services are preceded by contacting the Interoute Customer Contact Centre;

b. not install patches for the Operating System or Interoute Serviced Software unless expressly agreed by Interoute in advance;

c. be responsible for verifying the consequences of patches of the Operating System upon Customer applications (such as corruption, degradation or damage). Interoute is not responsible if a patch of the Operating System leads to corruption, degradation, damage to or a compromise of the Customer's applications or data. Interoute can provide a testing and or pre-production environment as part of the Solution if requested by the Customer.

Except for as set out in this Schedule 2N and Schedule 1, Interoute shall have no further liability to the Customer.