Business Services

PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE COMPUTING EXPRESS SERVICE

1.1 Definitions

All capitalized terms used but not defined herein will have the meanings set out in the General Conditions or in the Specific Conditions for Cloud Services.

"**Back End**" refers to a zone isolated from the internet and intranet, hosting services or application not accessible via the Internet,

"**DMZ (Demilitarized Zone)**" refers to a sub-network isolated by a firewall. This sub-network comprises machines located between an internal network (LAN – customer stations), an external network (Internet, usually) and applications exchange networks.

"**Front End**" refers to a front zone, hosting services or applications accessible from the Internet.

"**Hosting Platform**" refers to a set of facilities (room, cabling, power, UPS, etc.), hardware resources (server racks, physical servers) and software resources (operating system and software components) deployed by Orange to supply the Service.

"**Infrastructure**" refers to a set of resources (virtual machines, servers, firewall, load balancer, etc.) deployed by Orange to supply the Service.

"**Least Connection**" refers to a load balancing method that passes a new connection to the pool member or node that has the least number of active connections. The Least Connection method functions best in environments where the servers have similar capabilities. Otherwise, some amount of latency can occur.

"**MSCT**" or "**Management Service Change Toll**" means an Orange web portal which allows Customer to request and follow changes to the Service.

"**My Service Space**" or "**MSS**" means the Orange My Service Space web portal, which is a web portal that allows Customer to report and track Incidents, obtain information regarding the inventory of Customer's supported services, and monitor and obtain reports for certain supported services, using a login name and password provided by Orange when the supported service is implemented. MSS support is provided only in English.

"**NAS (Network Attached Storage)**" refers to an autonomous file server connected to a network, which main purpose is to store data as a centralized volume for heterogeneous client networks.

"**Reverse DNS**" means Reverse Domain Name System.

"**Round Robin**" refers to a load balancing method that passes each new connection request to the next server in line, eventually distributing connections evenly across the array of Virtual Machine being load balanced. Round Robin mode works well in most configurations, especially if the equipment being load balanced is roughly equal in processing speed and memory.

"**Self-management Portal**" means an Orange web portal, which allows Customer to manage their Infrastructure.

"**SSL (Secure Socket Layer)**" refers to a security protocol for exchanges on Internet, originally developed by Netscape (SSL version 2 and SSL version 3). It has been renamed as Transport Layer Security (TLS).

"**vCPU (Virtual Central Processing Unit)**" refers to a virtual component in a computer which helps executing IT programs.

"**Virtual Machine**" or "**VM**" refers to a software executable environment which emulates a hosting computer. Several Virtual Machines can be created in a single computer. Each User will have the illusion of having a complete computer while each Virtual Machine is isolated from the others.

"**VLAN (Virtual Local Area Network)**" refers to an isolated logical local IT network. Many VLANs may coexist on the same switch.

"**VPN (Virtual Private Network)**" refer to an extension of local networks ensuring the logical security provided by a local network. It is the interconnection of local networks via a tunneling technique using cryptographic algorithms.

1.2 Service Description

1.2.1 Overall Definition of the Service

The Flexible Computing Express Service (the "Service") is a Cloud Service which consists of a hosting service for IT infrastructure enabling Customer to manage their infrastructure with optimal flexibility and versatility.

The Service includes the implementation of the Service, the operation of the Hosting Platform and the provision and management of the Service in accordance with ITIL practices.

In accordance with the configuration defined in the Order Form and modified via the Self-Management Portal, the Service enables the Customer to set up the following functionalities:

- Hosting applications and data on the Infrastructures.
- Using the Infrastructures as:
  - a development, test and integration platform;
  - a preproduction platform;
  - a production platform; or
  - for hosting an application in SaaS mode (Software as a Service).

- Designing a secure architecture by partitioning services using security zones in the "secure architecture".
- Accessing its applications via Internet and/or VPN Intranet in a secured and efficient manner.
- Changing its architecture according to its requirements for:
  - Virtual Data Center resources (CPU power, RAM memory, Disk Space capacity);
  - Internet and/or VPN Intranet bandwidth; or
  - Secure architecture (Front-End, Back-end).

In addition, Orange will provide the following Infrastructure management services:

- Self-Management, operational and monitoring tools;
- Backup/restoration and storage tools; and
- Security services: updates for security patches, antivirus, security audits.

The network and security architecture (routers, firewalls, switches) of the Service is fully redundant, in "active/passive" mode.

1.2.2 Prerequisites

Orange recommends that Customer choose one of the following configurations for their computers, in order to manage resources and the Virtual Machine(s) via the Self-Management Portal:

Table 1: Operating System: Minimum Configuration for Browsers & Java Environments

Platform	Operating System	Minimum Configuration for Browsers & Java Environments
MS Windows	Windows 8 32 bit or 64 bit (with Desktop mode) Windows 8 Enterprise 32bit Windows 7 32 bit or 64 bit Windows 7 SP1 Enterprise 32bit Vista Enterprise SP1 32 bit or 64 bit XP Professional SP2 32 bit	Internet Explorer 7.0 Firefox 3.5 Oracle JRE 6
Mac	Mac OS X 10.8.x 32 bit Mac OS X 10.7.x 32 bit Mac OS X 10.6.x 32 bit or 64 bit Mac OS X 10.5.0 Mac OS X 10.4.3	Firefox 3.5 Oracle JRE 6
Linux	Ubuntu 11.x Ubuntu 10.x Ubuntu 9.10 OpenSuse 11.x OpenSuse 10.3	Firefox 3.5 Oracle JRE 6

1.2.3 Service Components

Customer has access to a Virtual Data Center (containing CPU power, RAM memory Disk Space Capacity, and included backup) and secure architecture resources (dedicated virtual firewall, load balancing). Every virtual server created by Customer is dedicated to Customer on a shared infrastructure (bandwidth, connection to the Hosting platform via the Internet and/or Intranet network, network and security equipment, server maintenance, premises, racks, storage, etc.).

The Service will be set up for Customer using standard or optional components, as selected by the Customer in the Order Form. Customer will identify in the Order Form and the Service Request Form:

- the components selected: resources of the Virtual Data Center, security elements in the secure architecture, backup elements, customer service, management portal, network connection and software elements;
- the initial configuration of the Service: standard and optional components to be included and the options which Customer wishes to subscribe to.

Customer can change the initial configuration of the Service via the Self-Management Portal for elements (automatically changed by the Customer) and via a change management tool for elements that can only be modified by Orange.

The physical server(s) used by Orange for the Service will remain the exclusive property of Orange. All hosted data and applications provided by Customer will remain the property of Customer.

1.2.3.1 Infrastructure Components

1.2.3.1.1 Standard Components

(a) **Virtual Data Center**

Orange will provide the Customer with access to a Virtual Data Center, including CPU Power, RAM memory, and one or two levels of hard drive capacity (Silver Disk Space capacity and Gold Disk Space capacity). Those resources are used to create the Virtual Machines.

The CPU power is set out in GHz values (processor power) and the RAM memory is set out in GB values.

Both type of Disk Space capacity (Silver and Gold) are provided with different performance levels and are divided into GB values (storage on the virtual machines). The same solution can have both Silver and/or Gold hard drive capacity.

Customer must define the reserved resources for their Virtual Data Center, as well as a maximum limit that the resources cannot exceed.

Customer can modify its reserved resources via the Self-Management Portal once a day and the maximum limit via the MSCT. The reserved resources may be exceeded for a day using the "CPU Power / RAM Memory Burst Option". For the purpose of this Service Description, 'a day' means 24-hours from 12:00 midnight Central Europe Time.

Customer can select amongst the following value for the reserved resources of the Virtual Data Center:

- CPU Power (GHz): 2, 4, 8, 12, 16, 32, 48, 64, 80, 112, 144, 192, 240, 288, 336.
- RAM Memory (GB): 2, 4, 8, 12, 16, 32, 48, 64, 80, 96, 128, 160, 192, 224, 256, 320, 384, 448.
- Silver disk space (GB) from 100 GB and by steps of 50 GB up to 25 TB.
- Gold disk space (GB) from 100 GB and by steps of 50 GB up to 25 TB.

Customer can select amongst the following maximum value for the definition of the Virtual Data Center limits:

- CPU Power (GHz): 2, 4, 8, 12, 16, 32, 48, 64, 80, 112, 144, 192, 240, 288, 336, 672.
- RAM Memory (GB): 2, 4, 8, 12, 16, 32, 48, 64, 80, 96, 128, 160, 192, 224, 256, 320, 384, 448, 896.
- Silver disk space (GB) from 100 GB and by steps of 50 GB up to 25 TB.
- Gold disk space (GB) from 100 GB and by steps of 50 GB up to 25 TB.

The disk spaces are based on several storage technologies and correspond to the nominative value +/- 3%.

The disk spaces may not exceed a usage rate of 98%.

(b) **Secure Architecture – Dedicated Firewall**

Orange will set up a secured Infrastructure with two levels of firewall.

The first pair is located at the upstream of the Hosting Platform with restrictive rules for analyzing and filtering traffic going through the platform and the VLANs.

A second pair of firewalls allows the Customer to define their own rules on dedicated virtual instances of the firewall.

Depending on the option subscribed by the Customer, this dedicated firewall gives access to up to 8 security zones, each containing VLANs related to Customer traffic (traffic VLAN), load balancing traffic (virtual VLAN) and Orange traffic (admin VLAN).

These security zones can be defined as:

- Front End security zones (internet zone , intranet/VPN zone with the VPN connection option);
- Back End security zones.

Each security zone contains: 32 private addresses of which 27 that can be used for Virtual Machines.

The Customer can configure its filtering rules using the Self-Management Portal.

The Customer must have the required knowledge and expertise to configure the firewalls. Any addition or modification made by the Customer to the filtering rules of the Virtual Machine is the Customer's sole responsibility. Orange will not verify any addition or modification made by the Customer to the filtering rules.

Orange will not be liable for loss or alteration of data relating to additions or modifications performed by the Customer to the filtering rules.

The Customer will be solely responsible for its network security policy and for the response procedures to security breaches.

Standard flow exception policy allows the flow of traffic between:

- the virtual machines in the infrastructure Flexible Computing Express;
- the internal network IP VPN client and the Virtual Machines hosted on offer Flexible Computing Express and located in Front End and Back End.
- the Internet and Virtual Machines located in a Front-End Internet.

The following graphic provides an understanding of the possible scenarios.

Table 2: Possible Scenarios Matrix

		Destination							
		Internet	**VPN**	**FE Internet**	**FE VPN**	**BE1**	**BE2**	**BE3**	**BE4**
Source	**Internet**		1	2	3	4	5	6	7
	VPN	8		9	10	11	12	13	14
	FE Internet	15	16		17	18	19	20	21
	FE VPN	22	23	24		25	26	27	28
	BE1	29	30	31	32		33	34	35
	BE2	36	37	38	39	40		41	42
	BE3	43	44	45	46	47	48		49
	BE4	50	51	52	53	54	55	56	

Key:

	Not authorized.
	Authorized from now on (but not open by default). Inconsistent with the activation of NAT VPN.
	Authorized (but not open by default).
	Not applicable.

Scenarios shown in box 9 and 16 each indicates that flows can be opened from the VPN to a VM on the Front-End Internet, and from a VM on the Front-End internet and the VPN.

If the Customer activates/uses the VPN NAT, the benefit from the opening of VPN flows will not be enjoyed.

Opening VPN flows increase risks for Customer's internal IT, and might impact the availability, integrity, and confidentiality of Customers' data and applications.

Therefore, Orange discourages to do this, based on the Orange Security Best Practices (that recommend using proxies). In doing so, the Customer removes one barrier in the protection of its internal corporate assets. By linking the internal systems to machines directly facing the Internet, the Customer will increase the IT risks presented to its business, including but not limited to: (a) misuse, abuse and/or infection of the corporate IT assets, (b) unintentional release or compromise of company confidential and/or sensitive data, (c) loss of data integrity or data destruction, (d) loss of availability or performance degradation of the internal systems, (e) compliance violation.

Nevertheless, if the Customer activates the VPN flows feature, it will be under its full responsibility, and the Customer acknowledges its full acceptance and undertaking of all risks implied by such an exposure and the burden of any counter-measures the Customer would implement. The Customer agrees and undertakes that no action, prosecution or other proceeding for damages will be pursued against Orange and/or its affiliates for any loss, damage, or adverse impact directly or indirectly suffered in connection with any escalated risk or incident due to this activation.

Orange is working to open all flow (Internet access from any security zone: boxes 3, 4, 5, 6, 7, 22, 29, 36, 43 and 50). When all the circumstances are met (information, security), Orange will keep the Customer informed of the new flow matrix policy and the associated risks.

(c) **Secure Architecture – Load Balancing**

Orange recommends that Customer implements a load balancing mechanism, by setting up redundant hardware for the Virtual Machines.

Virtual Machines availability and load balancing can be managed by the load balancer. The load balancing service (dedicated partition) is available to all secure zones.

Traffic management functionalities include:

- Intelligent load balancing (choice between two algorithms: Round Robin and Least Connection),
- IP source persistence.

NB: Customers who activate the load balancing mechanism must imperatively authorize ping requests on the Virtual Machines pooled by the load balancer. Otherwise, the load balancer will not be active on those Virtual Machines that will be considered as switched-off.

The maximum number of load balancing rules is maximum 10 in each security zones.

(d) **Applications Security**

Orange provides patches and application packages to the Customer on servers dedicated for that purpose (Microsoft and Linux servers).

These patches and application packages are intended for the update of Virtual Machines under MS Windows and Linux.

The Customer has remote access to these servers to get and install the patches, updates, and application packages provided by Orange.

The Customer is responsible for the installation (or non-installation) of those patches, updates and application packages on the Virtual Machines.

Orange validates those patches and application packages prior to providing them. If the result of the validation tests are not satisfactory as determined by Orange, Orange has the sole responsibility for the decision to provide those patches, and application packages.

Customer can also update its Virtual Machines by obtaining appropriate publicly available updates.

(e) **Virtual Machines backup**

Orange will use reasonable endeavors to back up the data installed on the Virtual Machines and the Silver and Gold hard drive capacity in accordance with the following policy:

- The retention period for backup is 14-day
- 1 total backup the first time
- 1 incremental backup daily

Notwithstanding the above, Customer acknowledges and agrees that a backup may not take place in accordance with the above policy because of the technology used for such back-ups and Customer must also perform its own backup procedures in order to avoid loss or damage to its data.

In the event of loss or damage to Customer data, the Customer can ask for the restoration of the latest backup of a Virtual Machine made by Orange, via the MSCT change tool. The restoration will be charged at the price in effect at the time of the request. Restored data shall be based strictly on the backup practice by Orange as described above.

(f) **Standard Customer Service**

Following the activation of the Service, the Standard Customer Service will organize a call of 30 minutes with the Customer to introduce itself and present the web portals.

The Standard Customer Service will contact Customer to review the billing elements of the first invoice issued to Customer for the Service. This call will last no longer than 30 minutes.

When Customer requests the possibility of importing or exporting data via the MSCT change management tool, it will be contacted by the Standard Customer Service.

The Standard Customer Service may contact Customer if necessary in the event of maintenance on the Hosting Platform.

Claim of any service credits as penalty for non-compliance with the Service Level Agreement will be addressed through the Standard Customer Service.

(g) **Customer Support Centre**

The Customer Support Centre is the point of contact for incidents reporting. The Customer Support Centre is available 24x7. Customer support is provided in English.

Orange will use reasonable endeavors to resolve incidents or provide a work-around.

Orange does not guarantee the resolution of incidents or the timeframe for providing an answer or a bypass solution.

Customer hereby confirms that it is knowledgeable in and fully understands Virtual Machine management concepts and related tools, and that it has the required skills in the field of Virtual Machine administration and related tools under whatever environment (MS Windows, Linux).

(h) **Managed Services Changes Tool – MSCT**

Orange will provide Customer access to the Managed Services Changes Tool – MSCT portal which allows Customer to send online requests for technical changes to be performed by Orange. Customer may access the MSCT portal using a secured link. Customer will connect to the MSCT portal with the logins provided by Orange. Customer will be responsible for the communication, utilization, and safeguarding of these logins. Customer will be responsible for any use or request made through the MSCT portal using the logins provided by Orange.

Two types of technical changes may be requested using the MSCT portal:

- Changes included in the monthly fees for the Service (as such changes are listed on the MSCT portal); and
- Changes chargeable at an extra fee (these changes are also listed on the MSCT portal). All fields must be fully and correctly completed by Customer when requesting a change.

The MSCT portal can only be used after activation of the Service.

Orange may also inform Customer of scheduled tasks on the Hosting Platform through the MSCT portal.

Any technical changes not listed on the MSCT portal must be requested through the Standard Customer Service.

(i) **My Service Space**

Orange will provide Customer access to My Service Space on any follow-up on incident tickets.

(j) **Reporting**

Orange will provide Customer with information regarding the usage of each of its Virtual Machines through the Self-Management Portal. Customer has access to a comprehensive range of information and statistics collected by Orange.

1.2.3.1.2 **Additional Components**

Customer may order the following optional components of the Service, either in the Order Form or through the Self-Management Portal after activation of the Service. These optional components are not included in the standard monthly Charges and are subject to additional monthly Charges payable by Customer.

(a) **Network Connection – Internet Connection**

The Internet connection includes:

- A redundant connection to the Internet at an Orange secured data center supervised on 24x7 basis.
- Bandwidth ranging from 1 Mbps to 1 Gbps in 1 Mbps increments.

The bandwidth is shared by all customers of Orange using the Service.

Customer is prohibited from making any inappropriate and/or excessive use of the Service.

Orange will notify Customer of any inappropriate and/or excessive use and request Customer to immediately cease such inappropriate and/or excessive use. Orange will be entitled to terminate the Service if Customer continues or repeats such inappropriate or excessive use following receipt of the notice sent by Orange, without prejudice of other right or remedy available to Orange.

For the purpose of this Clause, excessive use means any use of the Service exceeding the following thresholds:

- Use exceeding on average over 200% of the reserved quantity in Mbps over a given calendar month.
- Several uses in excess of five (5) times the reserved quantity in Mbps over a given calendar month.

The Parties agree that the readings established by Orange are conclusive of the thresholds.

(b) **Network Connection – Intranet VPN Connection – Business VPN Galerie**

Orange will provide Customer with the Intranet VPN service to connect the Service to Customer's VPN. Customer must have a Business VPN-type VPN access separately ordered from Orange.

The Intranet VPN connection includes:

- The connection of the Hosting Platform to Customer's MPLS VPN, so that the solution is seen by Customer as being part of a remote site on its private corporate network.
- The bandwidth between the said "remote site" and the VPN will range from 1 Mbps to 30 Mbps.

Any transfer volume exceeding the assigned bandwidth may cause disruptions to the Service. Orange will not be responsible for such disruptions. In the event of a dispute, the Parties agree that the measurements recorded in the Orange database will be conclusive of the excessive bandwidth use by Customer.

Customer will authorize ping requests on its VPN network in order to enable Orange, if required, to perform tests to diagnose a malfunction.

(c) **Public IP Addresses**

Orange does not set up any IP addresses for Customer during the Term of the Service. Customer may create, add, or remove public IP addresses using the Self-Management Portal. The maximum authorized number of public IP addresses is set at 3 per Virtual Machine, with a maximum of 10 public IP addresses at the same time. Customer may increase this limit by requesting a change through the MSCT portal. Additional IP addresses assigned by Orange are chargeable in accordance with the then standard charges schedule.

(d) **CPU Power / RAM Memory Burst Option**

The "CPU Power / RAM Memory burst" option allows Customer to exceed the resources reserved in the Virtual Data Center. The maximum extension will be twice the reserved value for the current day, as long as this is below the maximum threshold opted by the Customer in the Order Form or the subsequent change entered in the MSCT Portal.

Customer can subscribe to this option in the Order Form or through a change request (free option activation). Once subscribed, the option may be activated/deactivated at any time avoid excess use.

This option is charged on the basis of Customer average hourly use for each day.

(e) **Strong Authentication Authenticator Option**

The Strong Authentication option is a remote access administration service with strong authentication using SafeNet solution per user and includes:

- One or more Token RSA Software;
- A pair of redundant SSL Gateways;
- Strong Authentication Service (SAS).

(f) **VM Import/Export through USB Disks**

Virtual Machines can be imported/exported via physical media. The Customer can send external USB type drives to Orange containing one or more records ".OVA/OVF" each archive containing a Virtual Machine. The Customer can also send a blank external drive allowing it to export data. The maximum limit is 2 TB for different Virtual Machines accumulated on the USB drive. This service is called: Virtual Machine Import/Export via USB disk. The terms and prerequisites of this service are detailed in the Service Guide.

It is possible to combine import/export of multiple Virtual Machines on the same physical medium.

Imported VMs will be visible in the Customer's environment as private templates.

The VMs to be exported must be submitted by the Customer on an SFTP server, and then moved by Orange on a USB drive provided by the Customer, and will be sent to the address of the Customer.

(g) **VM Import/Export through the Network**

Virtual Machines can also be imported/exported through the network. Using the network the Customer can upload archives ".OVA/OVF" in a dedicated folder via SFTP SSL Gateway, each archive containing a Virtual Machine. The maximum limit is 50 GB for different Virtual Machines accumulated on the SFTP server. This service is called: Virtual Machine Import/Export via network. The terms and prerequisites for this service are detailed in the Service Guide.

Imported VMs will be visible in the Customer's environment as private templates.

The exported VMs is submitted by the Customer on an SFTP server and then made available to the Customer from the Internet.

(h) **Data Import/Export through USB Disks**

Data can be imported or exported via physical media. The Customer can send external USB disks containing such data archives to import a format as described in the Service Guide. The Customer can also send a blank external drive allowing it to export data. The maximum limit is 2 TB of data accumulated on the USB drive for import and export. These services are called: Import / Export data via USB drive. The terms and prerequisites of these services are detailed in the Service Guide.

The imported data is visible to the customer through a SFTP server accessible by Virtual Machines for 14 days after the transfer.

The data to be exported must be submitted by the Customer on an SFTP server, accessible by Virtual Machines, and then moved by Orange on a USB drive provided by the Customer, and will be sent to the address of the Customer.

(i) **Data Import/Export through the Network**

Data can be imported or exported via the network. The data must be submitted on an SFTP server accessible from its Virtual Machines and then the Internet. The maximum limit is 50 GB of data accumulated on the SFTP server. These services are called: Import / Export data via network. They are free and their terms and prerequisites are detailed in the Service Guide.

The imported data is visible to the Customer through an SFTP server accessed by Virtual Machines for 14 days after the transfer. The exported data is submitted by the Customer on an SFTP server, accessible by Virtual Machines, and then made available to the Customer from the Internet.

(j) **Reverse DNS**

Reverse DNS is the determination of a domain name that is associated with a given IP address using the Domain Name System (DNS) of the Internet. This option is available through MSCT.

1.2.3.2 Virtual Machines

Orange will allow Customer to create up to 200 Virtual Machines using the Self-Management Portal.

The Virtual Machines are created with the operating system chosen by Customer and configured with standard technical features. Customer may customize some of the technical features with the Self-Management Portal.

The Virtual Machines can be used as Front End or Back End, depending on the secured zone in which they are deployed.

Customer will access or manage the Virtual Machines or backup files with Software made available by Orange.

All Software are supplied "As Is" and Customer will have only such warranties, express or implied, if any, as provided by the third party Software licensor of such Software.

Orange will only provide such Software and applications indicated in the Order Form.

Orange will not be involved in the design, development, production, or maintenance of Customer’s Internet or Intranet website, Customer IT management and administration tools, or any applications services Customer installs on the Virtual Machines.

Orange does not provide Internet access and does not manage any such access.

The Orange Hosting Platform is accessible to the general public via the Internet network.

Orange will install agents to manage the Service (backup agent, antivirus agent) and will provide a set of patches, Microsoft service packs, bug fixes and Linux packs.

1.2.3.2.1 Virtual Machine Characteristics

Orange will provide virtualized servers using VMWare Vsphere technology. The technical characteristics of a VM are as follows:

- Reserved CPU power, maximum CPU power:
  - Minimum value to be reserved: 250 MHz
  - Maximum value to be reserved: 13.6 GHz
- Number of vCPU, CPU power being divided fairly by the number of vCPU:
  - Minimum value: 1 vCPU
  - Maximum value: 8 vCPU

- Reserved RAM Memory, maximum RAM Memory:
  - Minimum value to be reserved: 256 MB
  - Maximum value to be reserved: 64 GB
- Virtual disks with one Disk Space (Silver or Gold):
  - A virtual disk has a minimum of 1 GB and a maximum of 2 TB
  - A virtual machine has a limit of 2 TB of disk space

A VM may have minimum CPU power value and a maximum RAM memory value which can exceed the reserved value within the limit initially defined by the Customer.

1.2.3.2.2 **Antivirus**

The Virtual Machines include a Sophos Antivirus solution using MS Windows. Customer will have access to an administration console to manage its antivirus solution.

Orange will provide Customer with updates for this antivirus on a server remotely accessible by Customer. Customer is responsible for installing those updates on Customer's Virtual Machines.

1.2.3.2.3 **Operating Systems**

The Service includes the Debian and Ubuntu 32 bits and 64 bits operating systems in French and English.

Applications included in the Service are MS SQL Server 2005 32 bits and 64 bits Advanced Express; MS SQL Server 2008 64 bits Advanced Express; and MS SQL Server 2012 Standard 64 bits for 4, 6, or 8 vCPU per VM in French and English.

1.2.3.2.4 **Chargeable Operating Systems**

The following operating systems are also available (in French or English) at an additional charge: Windows 2003 32 bits Web Edition, Standard Edition and Enterprise Edition; Windows 2003 64 bits Standard Edition and Enterprise Edition; Windows 2008 64 bits Web Edition, Standard Edition, Enterprise Edition, and Windows 2012 64 bits Standard Edition.

Windows Server RDS (Remote Desktop Services) license must be requested through MSCT and is charged per User.

1.2.3.2.5 **Backup and Restoration**

Virtual Machines are backed up as described in Clause 1.2.3.1.2(e) above. Those Virtual Machines may be restored by Orange following a request made using the MSCT provided for Customer by Orange.

1.2.3.3 **Self-Management Portal**

Customer will administer its Virtual Data Center, secure architecture, Virtual Machines and other components of the Service using the Self-Management Portal, accessible via strong authentication.

Orange will provide Customer with software tokens and logins at the date of installation of the Virtual Machines. Customer undertakes not to disclose these logins to any person not authorized to use the Service. Customer will be solely responsible for the use of the logins provided by Orange.

Customer may access its Virtual Machines via SSL. After authentication, Customer may connect to its Virtual Machines and perform the actions defined in the Self-Management Portal remotely.

Customer cannot modify the logins to its Virtual Machines or the Self-Management Portal.

In the event of loss or theft of the logins Customer must inform the Customer Support Centre as soon as possible, and the Customer Support Centre will send Customer new logins.

1.3 Order Term and Termination

1.3.1 Term and Termination

Each Order will have a Service Term of 3 months, 12 months, or 36 months, as chosen by Customer, following the date of activation of the Service.

The Extended Term for each Order will be the same as the Service Term and each Order will be automatically renewed for successive Extended Terms, unless terminated earlier pursuant to Clause 7.4 of the General Conditions.

Each Party may terminate an Order by giving the other Party at least a) 90 days' notice for a Service Term or Extended Term of 12 or 36 months; or b) 30 days for a Service Term or Extended Term of 3 months, prior to the end of the Service Term or Extended Term as applicable.

1.3.2 Termination for Convenience

1.3.2.1 **Termination of the Order**

Customer will be entitled to terminate an Order at any time for convenience, subject to the payment of the following early termination fees:

- For a Service Term and Extended Term of 3 or 12 months: USD549 for each month of the remaining period of the then current Service Term or Extended Term; or
- For a Service Term and Extended Term of 36 months: a) USD549 for each month of the remaining period of the then current Service Term or Extended Term; and b) if Customer terminates the Order before the 24th month of the Service Term or Extended Term, Customer will reimburse Orange the difference between the fees actually

paid by Customer from the beginning of the Service Term or Extended Term (as applicable) and the fees that would have been payable by Customer for; (i) a 3-month Service Term if terminated before the 12th month of the Service Term or Extended Term, or (ii) a12-month Service Term if terminated after the 12th month of the Service Term or Extended Term, as applicable.

1.3.2.2 **Termination of Optional Components**

Customer will be entitled to terminate each optional component by providing Orange at least (a) a 90 days' notice for a Service Term or Extended Term of 12 months or 36 months or (b) a 30 days' notice for a Service Term or Extended Term of 3 months, prior to the end of the Service Term or Extended Term as applicable. Otherwise optional components will be automatically extended for each successive Extended Term.

In addition, Customer will be entitled to terminate an optional component at any time for convenience, subject to the payment of all corresponding fees which would have normally be due until the end of the then current Service Term or Extended Term.

1.3.3 **Conditions of Termination**

Upon receipt of the notice of termination, Orange will acknowledge the termination by email to Customer's main administrator. A follow up mail will be sent 28 days before the anticipated date of termination to notify the suspension of the Service with limited rights on the Self-Management Portal. A last mail will be sent 14 days later to notify the actual termination of the Service. Customer may cancel the termination or request a 14 days extension of the Service at any time prior to this last email, by contacting the Standard Customer Service.

The Service will be charged until the day of its actual termination.

1.4 Limitations of Use

Customer will not analyze, disassemble, or modify the configuration of the Hosting Platform, its structure or any files therein. Customer is only permitted to install, update, or delete files and folders on its website and/or the applications hosted on its Virtual Machines.

Customer will not perform or attempt to perform any intervention on third-party Virtual Machines and/or websites hosted on the Hosting Platform, and/or any intrusion or attempted intrusion into Orange information systems. Any such action will be considered a material breach of the Agreement.

Customer acknowledges and agrees that all Software used on the Hosting Platform and the Virtual Machines are technically complex and cannot be tested in such a way as to cover every possible use. Customer acknowledges and agrees that the Hosting Platform and the Virtual Machine will not be error free or may be non-available.

Customer is fully aware of the bandwidth limitations and of its shared use for the connection to the Hosting Platform. Orange reserves the right to deploy any software required to monitor and limit the use of the bandwidth.

Customer will actively cooperate with Orange to maintain its tools at the best possible level of quality. Customer will follow all instructions from Orange and will promptly perform any operation recommended by Orange, including the reinstallation and/or reconfiguration of the Service or installation of updates to software and/or hardware. Customer will be advised of said recommendations by the Standard Customer Service or any other means as deemed appropriate by Orange.

Orange reserves the right to substitute the Virtual Machine(s) allocated to Customer if Orange deems it necessary in its reasonable opinion. Orange will endeavor to provide Customer as much notice as reasonably possible and will, in cooperation with Customer, organize the transfer of Customer's solution onto the new Virtual Machine.

If Customer does not cooperate with Orange as reasonably required, Orange reserves the right to either terminate the Service or suspend the Service until such time Customer's use of the Service is in compliant.

Orange reserves the right to interrupt access to the Hosting Platform or the Virtual Machines to perform repairs, maintenance and/or improvement interventions in order to ensure proper operation of the Service. Orange will use reasonable endeavors to inform Customer to the extent possible, about such intervention and their duration. Orange will perform maintenance operations at times when Virtual Machines are the least used by Customer, except in the event of emergency maintenance.

Customer remains solely responsible for its network's security policy and for its response procedures to security violations. Orange will use reasonable endeavors to prevent unauthorized access to the network and to Customer files, and will help Customer detect any potential security breaches.

Customer is solely responsible for the content of any postings, data, or transmissions (collectively, the "Content") using the Service, or any other use of the Service by Customer or any of its authorized user, person or entity that Customer permits to access the VM and/or the Service. Customer represents and warrants that neither it nor any of its authorized user, person or entity will use the Service, whether directly or indirectly, for unlawful purposes (including infringement of Intellectual Property Rights, misappropriation of trade secrets, wire fraud, invasion of privacy, pornography, obscenity, defamation, illegal chat lines or illegal use) or to interfere with, or disrupt, other network users, network services, or network equipment. Disruptions include distribution of unsolicited advertising or chain letters, repeated harassment of other network users, wrongly impersonating another user, falsifying one's network identity for improper or illegal purposes, sending unsolicited mass emailings, propagation of computer viruses, and using the network to make unauthorized entry to any other machines accessible location, via the network. Orange may suspend or terminate any or all Service immediately, without prior notice to Customer, if Orange believes in good faith, that Customer or any other person or entity is utilizing the Service for any such illegal or disruptive purpose. Customer will defend, indemnify, and hold harmless Orange and its Affiliates from and against

all Losses arising out of or relating to any and all claims by any person or entity relating to use of the Service, including use of the Service without consent of Customer or as otherwise stated above.

1.5 Termination Assistance Services

Upon expiry or termination of an Order (other than as a result of Customer's breach), Customer may request to Orange by written notice (registered letter with acknowledgement of receipt) to provide termination assistance services for the Service for a period not to exceed the end of the termination notice period (the "**Termination Assistance Period**"), unless otherwise agreed upon by Orange.

The standard termination assistance services will consist of:

- The supply of technical information about the Service architecture, except any information considered by Orange as know-how owned by Orange,
- The participation in meetings to determine and prepare for the migration of Service, subject to a maximum of one (1) meeting per month.

If Customer wishes to receive additional termination assistance services from Orange, Orange will provide a quote for such additional termination assistance services, specifying the charges and conditions for such assistance and any necessary material and physical installations.

Customer will remain solely responsible for the replacement of third party service provider.

Customer will supply all the necessary technical and required resources at its own costs for the migration of the Service.

If Customer requests the assignment of any Software license at the end of the Service, such assignment will be subject to the relevant third-party licensor prior agreement and terms and conditions to be agreed by the Parties.

1.6 Geographic Availability

The Service is available worldwide. The Data Centers are located in France and Singapore. Customer can opt for either of the locations for the Service.

1.7 Technical Restrictions

Customer will take all necessary technical precautions for the use of the Service and will ensure the compatibility of its website and/or applications with the Service, the Virtual Machines, the system resources, the software, and the technical restrictions of the Orange platform.

Customer will ensure that its use of the Service will not cause any excessive load on Orange servers.

Customer will comply with standard programming techniques, as well as all instructions given by Orange for the development its website.

Customer will not do anything which may impact the configuration of the Hosting Platform, its security or its operation, or may affect the Infrastructure assigned to Customer.

Customer will comply with the conditions of use, including but not limited to the following:

- VMware services, among other things, must not be stopped.
- No entry in the system configuration must be deleted and especially the /etc/hosts file.
- No entry must be deleted in the routing table.
- Preconfigured IP addresses and system hostname must not be modified.
- No modification must be done on the following repertories:
  - /usr/lib/vmware-tools.
  - /etc/vmware-tools/.
- No modification must be done on preconfigured network interfaces in the image of MS Windows Server or Linux provided with the virtual machine all distribution and edition combined.
- No change/deletion of partition table of virtual machine except for non-allocated space.
- No change/deletion in peripheral manager (change/removal of drivers).
- No change/deletion of the following user accounts:
  - Administrator.
  - SophosSAU.
- No change/deletion of the following user groups:
  - Sophos Administrator.
  - SophosOnAccess.
  - SophosPowerUser.
  - SophosUser.
- No change to "Started" state of the following services:
  - Automatic Updates.
  - DNS Client.

    - Event Log.
    - Logical Disk Manager.
    - Sophos Agent.
    - Sophos Antivirus.
    - Sophos Auto Update Service.
    - VMWare physical disk Helper Service.
    - VMWare Tools Service.
- No change/deletion of register keys associated with:
    - VMWare.
    - Sophos Antivirus.
    - Windows Update.
- No change/deletion in program manager of:
    - CDP Open Transaction manager.
    - Sophos Antivirus.
    - Sophos Auto Update.
    - Sophos Remote Management System.
    - VMWare Tools.
- No change/deletion of the following directories in "Program Files":
    - AVS.
    - Sophos.
    - VMWare.
- No change/deletion of libraries associated with:
    - VMWare.
    - Sophos Antivirus.
    - Windows Update.
- No change/deletion of network conf of VM interfaces:
    - Default IP addressing/masks/routes.
- No change/deletion of initially defined static routes.
- No deletion of system files.
- No deletion of "Event Viewer" logs.

Orange will not be responsible for any Service malfunction and/or loss of data caused by non-compliance with these conditions of use.

Orange will not be responsible if the configuration of the Service chosen by Customer is not sufficient to address its needs in term of connections or requests or exceed Customer forecasts.

Orange reserves the right to suspend or terminate the Service in the event of repeated non-compliance by Customer with the technical restrictions specified in this Clause 1.7.

END OF SERVICE DESCRIPTION FOR FLEXIBLE COMPUTING EXPRESS SERVICE