1 SERVICE DESCRIPTION FOR FLEXIBLE COMPUTING PREMIUM SERVICE

1.1 Definitions

All capitalized terms used but not defined herein will have their meanings set out in the Master Services Agreement and in the Specific Conditions for Orange Flexible Computing Global Service.

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

"**Change Catalog**" refers to the Changes that can be requested by Customer as part of the Service.

"**Customer Application**" refers to all Customer's application hosted on Customer Platform.

"**Customer Platform**" is composed of infrastructure components and management services hosted in an Orange managed Data Center.

"**Customer Solution**" is composed of Customer Platform and Customer Application.

"**DMZ**" a DMZ is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger untrusted network.

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

"**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.

"**Low Level Design**" refers to the document that details the technical specification of Customer Solution.

"**Operational Acceptance Testing**" or "**OAT**" designates the testing conducted to close the build phase of the project. As soon as Customer Solution is deployed, the Operational Acceptance Testing phase starts.

"**Operational Service Verification**" or "**OSV**" designates the verification of Customer Solution before moving to operational mode.

"**Project Kick-off Meeting**" or "**PKM**" first project meeting between Customer and Orange, which will be held at the start of the deployment phase.

"**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 Machines being load balanced.

"**Service Request Form**" refers to the document that describes the components of Customer Solution together with their management services, and the service levels.

"**Technical Acceptance Test**" designates the milestone for the validation of Customer Platform deployment phase, the process of which is as set out in Clause 1.3.3 below.

"**Virtual Datacenter**" or "**VDC**" The Virtual Datacenter (VDC) provides the resources, CPU power, RAM memory, and disk space, needed to create Virtual Machines and back them up.

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

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

"**VPN**" or "**Virtual Private Network**" refers to an extension of local networks insuring 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 Premium Service (the Service) is a Cloud Service that allows Customer to create a flexible, managed infrastructure solution according to Customer requirements, based on a catalog of industrialized infrastructure components and management services.

1.2.2 Definition of the Service

The Service allows Customer to:

- Host applications and data on a virtualized infrastructure and on dedicated physical servers for applications that are non-virtualisable with different management services.
- Implement one or more platforms in order to respond to the following use cases, such as:
  - Development, test and integration platform,
  - Pre-production platform,

    - Production platform,
    - Hosting of software company application in SaaS (Software as a Service) mode.
- Partition services using DMZ and VLAN security zones,
- Access services and applications via the Internet and/or intranet VPN,
- Scale the architecture according to Customer needs in terms of:
    - resources (CPU, RAM, disks),
    - network bandwidth for Internet and/or intranet VPN,
    - security architecture.
- Benefit from commitments on Quality of Service as described in the document Service Level Agreement for Flexible Computing Premium, such as:
    - Guaranteed Service Availability Rate (GSAR).
    - Guaranteed Time To Restore (GTTR).
    - Guaranteed Time To Change (GTTC).
- Benefit from management services:
    - Managed OS:
        - includes supply and management of Customer's underlying infrastructure, for example, servers, storage, security,
        - supply of operating systems and license management as per the operating systems listed in the Charges Schedule,
        - supply user accounts with limited right, as defined by Orange during Customer Platform deployment phase,
        - patch management and operating systems monitoring.
    - Middleware monitoring:
        - includes Managed OS,
        - 24x7 monitoring of a middleware managed by Customer and 24x7 application of production instructions supplied by Customer if a monitoring alarm is reported.
    - Managed middleware:
        - includes Managed OS,
        - supply and installation of middleware and management of associated licenses, as per the middleware listed in the Charges Schedule,
        - patch management and 24x7 monitoring of middleware,
        - supply an administration tool for managing and updating application content.
    - Application outsourcing:
        - includes Managed OS,
        - supply and installation of middleware and management of associated licenses, as per the middleware in the Charges Schedule,
        - patch management and 24x7 monitoring of middleware,
        - deployment of Customer Application versions and content.

Orange supplies and operates a set of tools and services for infrastructure management, such as:

- Tools for administration, operation and monitoring,
- Tools for backup/restore and storage,
- Security services: n-tier security architecture based on DMZ, updates to security patches, antivirus and security audits.

1.2.3 Service Content

The Service consists of:

- the provision of hardware and software resources including one or more virtual servers and dedicated physical servers, configured to host Customer Application,
- Operating the Service,
- Managing and supplying the Service in compliance with Information Technology Infrastructure Library (ITIL) ITILv3 practices.

Each virtual or physical server is dedicated to Customer on a shared and partitioned infrastructure, for example, bandwidth, connection to the platform via the Internet and/or intranet, network and security equipment, server maintenance, premises, bays, storage.

The server or servers used by Orange for supplying the Service remain the exclusive property of Orange. The hosted data remains the property of Customer.

The charges applicable to Customer during subscription to the Service are those specified in the Charges Schedule.

The deployment of the Service including the services chosen by Customer and their connections to the Internet and/or the Intranet is performed by Orange.

As a minimum, Customer must have:

- a Virtual Datacenter with a minimum of 2 GHz, 2 GB of RAM, and 100 GB of storage,
- a dedicated firewall with at least 2 security zones,
- a dedicated load-balancer,
- a software authentication system,
- an Internet connection of a minimum of 1 Mbps,
- a security server, managed by Orange, hosted in Customer's Virtual Datacenter,
- an FTP area for file exchange between the virtual and physical servers of Customer's architecture.

1.2.3.1 **Infrastructure Components**

(a) **Virtual Datacenter**

Customer accesses resources presented in the form of a Virtual Datacenter, including CPU power, RAM memory, and one or two types of disk space (Silver disk space and Gold disk space). These resources are used to create Virtual Machines.

The CPU power is measured in Gigahertz (GHz) values while the RAM memory is measured in Gigabyte (GB) values.

Both types of disk space, Silver and Gold, are offered with different performance specifications and are measured in Gigabyte (GB) values (storage for Virtual Machines). For a given solution, it is possible to have both Silver and/or Gold disk spaces.

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

Customer can modify the reserved resources and the maximum limit once a day through a change request via the Managed Services Changes Tool (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 among the following values for the reserved resources of the Virtual Datacenter (collectively the Reserved VDC Values):

- CPU power (in GHz): 2, 4, 8, 12, 16, 24, 32, 48, 64, 80, 112, 144, 192, 240, 288, 336.
- RAM memory (in GB): 2, 4, 8, 12, 16, 24, 32, 48, 64, 80, 96, 128, 160, 192, 224, 256, 320, 384, 448.
- Silver disk space (in GB) from 100 GB configurable in increments of 50 GB up to 10 TB.
- Gold disk space (in GB) from 100 GB, configurable in increments of 50 GB up to 10 TB.

Customer can select among the following maximum values for the definition of the Virtual Datacenter limits (collectively the Maximum VDC Values):

- CPU power (in GHz): 2, 4, 8, 12, 16, 24, 32, 48, 64, 80, 112, 144, 192, 240, 288, 336, 672.
- RAM memory (in GB): 2, 4, 8, 12, 16, 24, 32, 48, 64, 80, 96, 128, 160, 192, 224, 256, 320, 384, 448, 896.
- Silver disk space (in GB) from 100 GB configurable in increments of 50 GB up to 10 TB.
- Gold disk space (in GB) from 100 GB configurable in increments of 50 GB up to 10 TB.

The disk spaces correspond to the nominative value +/- 3%.

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

In the context of the Service, Customer can define between 1 and 6 Virtual Datacenters and a maximum of 216 servers (Virtual Machines or physical servers) in Customer Platform.

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

Orange allows Customer to exceed the CPU power and RAM memory reserved for a Virtual Datacenter if Customer activates the CPU power and RAM memory burst option. The maximum authorized overrun corresponds to twice the Reserved VDC Values for the current day, but in no event more than the Maximum VDC Values.

This option must be subscribed initially or by a change request. This option is charged on an hourly usage basis.

(c) **Virtual Machines**

Orange offers Virtual Machines using the VMWare VSphere technology. The technical characteristics of a VM are as follows:

- Reserved CPU power, maximum CPU power:
  - Minimum value: 250 MHz.
  - Maximum value: 13.6 GHz. (8 vCPU * 1.7 GHz).
- Choice of the number of vCPUs, the CPU power being divided equally by the number of vCPUs (1, 2, 4, 6 or 8 vCPUs):
  - Minimum value: 1 vCPU.
  - Maximum value: 8 vCPUs.
- Reserved RAM memory, maximum RAM memory:
  - Minimum value to reserve: 256 MB.
  - Maximum value to reserve: 64 GB.
- Virtual disks within a single disk space (Silver or Gold):
  - A virtual disk has a minimum of 1 GB and a maximum of 2 TB.
  - A VM has a limit of 2 TB of disk space.

A Virtual Machine can have maximum CPU Power and RAM memory values that can be greater than its reserved CPU Power and RAM.

A Virtual Machine may occasionally automatically exceed the capacity reserved for it in CPU power and RAM memory resources. It draws from the overall resources of the Virtual Datacenter that are not assigned to other machines, within the limits defined by Customer.

Virtual Machines back up:

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:

- 1 complete backup following the creation of the VM.
- 1 incremental daily backup.
- the backup retention period is by default set to 14 days. It is possible to define a different retention period for all VMs in one Virtual Data Center. Higher retention period will be charged additionally.

In case Customer's data is lost or destroyed and upon change requests from Customer, the last backup of a VM can be restored. The restore thus allows a VM to be restored to the state that it was at the time when it was backed up. The restore operation is invoiced at the price in use on the day of the request. Restored data shall be based strictly on the backup practice by Orange as described above.

(d) **Physical Servers**

Orange proposes Customer to host and manage servers that are non-virtualisable. The management of physical servers is available for Windows and Linux environments. Orange offers 3 ranges of servers listed in the Charges Schedule.

(e) **Dedicated Virtual Firewall**

Orange provides two levels of firewalls: The first pair of dedicated virtual firewalls upstream of the platform with restrictive rules for analyzing and filtering traffic passing through the platform and the VLAN. The applied configuration is of type all traffic not expressly allowed is prohibited.

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

This dedicated virtual firewall provides the ability to configure up to 8 security zones providing up to 216 private IP addresses, each one with a VLANs related to Customer traffic (traffic VLAN), a VLAN for load-balancing traffic (virtual VLAN) and a VLAN for Orange traffic (administration VLAN).

These security zones can be of type: Back End, Front End Internet, and Front End Intranet (VPN). Orange shall not be held liable for any loss or damage to data as a result of an addition or modification of filtering rules performed at Customer's request. Customer remains responsible for the security policy of their network and procedures for reacting to security breaches.

(f) **Dedicated Virtual Load Balancer**

Customer defines their own load-balancing rules, based on redundant Virtual Machines.

The availability of VM load distribution may be managed by the load balancer. The load balancing service (dedicated partition) is available for all the security zones.

The traffic-management functionalities include:

- intelligent load balancing (choice between 2 algorithms: Round Robin and Least Connection),
- IP source persistence.

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

(g) **Network Connection – Internet Connection**

The Internet connection service is intended to supply the connection to the Internet and the bandwidth for a hosting solution.

The functional elements offered are as follows:

- A redundant Internet connection on a secured Datacenter supervised on a 24x7 basis,
- A quantity of bandwidth varying from 1 Mbps to 1 Gbps, by increments of 1 Mbps.

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

Orange will notify Customer of any excessive use and request Customer to immediately cease such excessive use. Orange will be entitled to terminate the Service if Customer continues or repeats such 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:

- exceeding on average 200% of the reservation in Mbit/s on a given month,
- several uses in excess of five (5) times the reserved quantity in Mbit/s during a given calendar month.

The Parties agree that the reading established by Orange is conclusive of the thresholds.

(h) **Network Connection Option – Intranet VPN Connection**

Orange offers the intranet VPN service to Customer, to connect the Service to Customer's VPN. Customer must have a VPN access of Business VPN type.

Customer's VPN connection service is intended to supply:

- The connection of the hosting platform to Customer's MPLS VPN, so that the solution is seen by Customer, as forming part of a remote site on its private enterprise network,
- The bandwidth between the remote site and the VPN ranges from 1 Mbps to 50 Mbps.

Any transfer volume exceeding the bandwidth allocated 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 technical database shall be conclusive of the excessive bandwidth use by Customer.

The Customer will authorize Ping requests on its VPN network to allow Orange, if necessary, to perform tests to diagnose malfunctions.

(i) **Public IP Addresses**

Orange provides public IP addresses. These addresses are exclusively owned by Orange. The maximum authorized number of public IP addresses is set at 3 per Virtual Machine or dedicated Physical server.

(j) **Shared SMTP Gateway**

Orange offers as an option, an outgoing mail relay service towards the Internet for requirements related to Customer Application. All outgoing emails will be processed by antivirus software.

(k) **Active Directory Server**

According to the number of servers and/or the number of customer administrators, Orange reserves the option to implement a directory server.

The CPU/RAM/Storage resources for this server are taken from the resources of Customer's Virtual Datacenter.

(l) **Security Server**

The Service includes a security server to address the obligation of the parties on logs as defined in the Clause 1.7.1 below.

The CPU/RAM/Storage resources for this server are taken from the resources of Customer's Virtual Datacenter.

This server allows the centralization and provision of the logs which will be stored in the security server for one (1) week from the time the log is created.

The logs for which Customer is responsible for (as that outlined in Clause 1.7.1 below) must be archived by Customer.

The security server shall be installed in a Back End zone.

The logs are accessed by Customer, in read-only mode, via FTP (File Transfer Protocol).

(m) **FTP Server**

This server is provided by Orange, located outside the Customer Platform, and is accessible by all VM and dedicated physical servers.

(n) **Administration Server for Administration Tool**

The administration tools service is intended to supply a VM on which Customer has the option to administer and manage their platform, whether it is under Windows 2008 or Linux.

The administration tools are installed on Windows Server 2008 OS and provided to Customer with limited access (restricted usage). Customer may not install their own tools.

This service allows Customer to:

- carry out all the administration tasks delegated to them for the different Services under Windows and Linux,
- supervise the Services using standard Windows tools or otherwise: event logs and performance counters,
- administer the Services through specific tools (as indicated in the Charges Schedule. This Service is supplied exclusively in the Managed middleware management service.

(o) **Strong Authentication by the Software Authenticator**

The remote-access to the administration platform requires a RSA SecurID software token per user: this is a software authenticator.

The provided functional elements are as follows:

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

1.2.3.2 **Management Services**

Orange allows Customer to design its Service in a flexible way according to their needs.

The Management services provided by Orange are modular and Orange can offer all or part of the Management services described here after.

(a) **Managed OS**

For this service, Orange undertakes to:

- supply operating system templates (as per the Operating systems in the Charges Schedule), including:
  - an antivirus (according to the OS).
  - a backup agent.
  - a supervision agent (according to the OS).
- manage the license and the media (according to the publisher).
- server deployment (virtual or physical), using the configuration recommended by Orange.
- daily backup of the files system.
- security monitoring.
- patch management (see Clause 1.4.10 Management of Patches and Scheduled Tasks).
- 24x7 supervision.
- incident management.
- give access to the system logs managed by Orange.
- supply usage indicators (for example, CPU, RAM, hard disk).

With Managed OS service, Customer can ask for administration rights on the operating system for a limited period of 7 calendar days. During this period, the OS monitoring, the SLA and the patch management by Orange are suspended. The SLA will apply again 7 calendar days after the return of the administration rights to Orange.

Orange proposes as an option, the installation of middleware as per the middleware listed in the Charges Schedule together with the management of the associated license.

(b) **Middleware Monitoring**

This service is based on the Managed OS service. It covers the monitoring of the middleware.

For this service, Orange undertakes to:

- manage the license of the middleware supplied by Orange as per the middleware listed in the Charges Schedule.

- monitor the middleware whether or not supplied by Orange on a 24x7 basis for the:
  - absence/presence of a process (min/max instance number).
  - absence/presence of a file.
  - presence of a string in a file.
- manage incidents on the middleware whether or not supplied by Orange, based on operational instructions provided by Customer.
- give access to the system logs managed by Orange.

Orange reserves the possibility to suspend the OS and middleware monitoring in case Customer does not take corrective actions to solve an incident.

(c) **Managed Middleware**

This service is based on the Managed OS service. It covers the management of middleware as per the middleware listed in the Charges Schedule.

For this service, Orange undertakes to:

- supply the Managed OS (without access for Customer).
- manage the license and media of the middleware supplied by Orange.
- deploy the middleware supplied by Orange.
- supply a management tool for some middleware.
- perform a daily backup of all data and configurations.
- perform security monitoring of the middleware supporting Customer Application.
- perform patch management (see Clause 1.4.10 Management of Patches and Scheduled Tasks).
- monitor, 24x7, the middleware supplied by Orange.
- perform incident management.
- give access to the system and middleware logs managed by Orange.
- supply usage indicators on the middleware.

(d) **Application Outsourcing**

This service based on the Managed OS service. For this service, Orange undertakes to:

- supply the Managed OS (without access for Customer).
- manage the license and media of the middleware supplied by Orange.
- deploy the middleware supplied by Orange.
- deploy Customer Application.
- perform a daily backup of all data and configurations.
- perform security monitoring of the middleware supporting the application.
- perform patch management (see Clause 1.4.10 Management of Patches and Scheduled Tasks).
- perform 24x7 technical supervision of Customer Application (excluding the functional monitoring of business rules).
- perform incident management.
- give access to the system and software logs managed by Orange.
- supply usage indicators for the middleware and for the deployed Customer Application.

This service requires that Customer Solution includes a pre-production environment for patches validation before applying them on Customer Platform.

Note that this service excludes third-party maintenance of Customer Application, which remains the responsibility of Customer.

1.2.3.3 Customer Application Service Deployment

The Parties' respective responsibilities in regard to the Customer Application Service Deployment are dependent on the type of management service opted for by Customer, which details are set out below:

(a) **Customer Application Service Deployment under managed OS, middleware monitoring and managed middleware management services**

The Customer Application Service Deployment will be carried out by the Customer. However, the Customer may opt to assign to Orange the implementation of certain of the deployment activities that are mutually agreed upon. Customer Application Service Deployment under application outsourcing management service.

The Customer Application Service Deployment will be carried out by the Customer with Orange performing the operations based on the prerequisites, installation procedures agreed upon between the Parties and the input data provided by the Customer.

1.3 Service Deployment

The Parties agree that the Date of Acceptance for Customer Solution corresponds to the date on which Operational Service Verification is completed.

The deployment of Customer Solution consists of six (6) phases set out below.

Prerequisite:

The Service Request Form, technical specification, and instructions for Customer Solution must be completed and validated by Customer and Orange by the time of the Project Kick-off Meeting. This validation is a prerequisite for deployment.

1.3.1 Customer Solution Design

This phase is intended to consolidate the prerequisites of Customer Solution by completing the Low Level Design and validating the associated workload and planning. This phase is completed when the Low Level Design has been validated by Orange and Customer.

1.3.2 Customer Platform Build

This phase corresponds to the build of the Customer Platform. During this phase the infrastructure components are deployed as per the Service Request Form and Low Level Design.

1.3.3 Technical Acceptance Test

When Orange has completed Customer Platform build, Customer must then approve the Technical Acceptance Test, by signing the Technical Acceptance Test minutes sent by Orange.

If Customer signs the minutes without qualification, the invoicing associated with Technical Acceptance Test will be triggered by Orange.

Two types of qualifications may be issued by Customer:

- minor qualification: where Customer wishes to change an element of their technical solution, without detecting any technical incompatibility; or
- major qualification: where Orange or Customer detects a proven or potential incompatibility problem between one or more elements of the technical solution. This may be related to an inadequate upstream analysis of the solution or a lack of information from Customer.

Orange undertakes to address and resolve the qualifications. The qualifications are resolved when Customer approves and signs the re-submitted Test Acceptance minutes. Notwithstanding the above, Technical Acceptance Tests will be deemed to have taken place if there shall be no response from Customer (Deemed Acceptance) or on occurrence of either of the following:

- three (3) working days following the resolution of minor qualifications as notified by Orange;
- five (5) working days following the resolution of major qualifications as notified by Orange.

Upon Acceptance or Deemed Acceptance, invoicing will commence for the following Charges:

- setup Charges for the Customer platform (the full sum on Technical Acceptance Test).
- usage Charges for CPU/RAM/Disk (billed monthly in arrears).
- monthly Charges for licenses (billed monthly in arrears).
- setup Charges and monthly subscription Charges for the dedicated physical servers (billed monthly in advance).
- setup Charges and monthly subscription Charges for additional Services, if applicable (billed monthly in advance).

1.3.4 Customer Application Deployment

This phase corresponds to the installation and configuration of Customer Application on Customer Platform, according to the Low Level Design validated by Customer.

1.3.5 Operational Acceptance Testing

The Operational Acceptance Testing completes the deployment of Customer Solution. It includes the deployment of up to two patches for Customer Application if required.

Any additional patch or complete re-deployment of Customer Application due to a request by Customer will be chargeable to Customer in accordance with the Change Catalog. In this case, Customer acknowledges and accepts that Orange cannot give undertakings concerning the availability of its resources and therefore the deadline for delivery of Customer Application may need to be adjusted.

On completion of the Operational Acceptance Testing:

- Customer will approve the Operational Acceptance Testing by signing the Operational Acceptance Testing minutes without qualification;
- or Customer will issue either minor or major acceptance qualification. Two types of qualifications may be issued by Customer based on the technical solution defined in the Low Level Design:
  - minor qualification: where Customer wishes to change an element of the Customer Application, without detecting any functional incompatibility; or
  - major qualification: where Orange or Customer detects a proven or potential incompatibility problem between one or more elements of the Customer Solution. This may be related to an inadequate upstream analysis of the solution or a lack of information from Customer.
- Orange undertakes to resolve the qualification as soon as possible, for example by deploying a first patch.

On being notified by Orange of the resolution of the qualification, whether or not a patch is deployed:

- either Customer signs the Operational Acceptance Testing minutes without reservation;
- or Customer refuses to sign the minutes, issuing a major or minor reservation: they must then state this reservation on the minutes and Orange undertakes to lift it as soon as possible, for example by deploying a second patch.

The above process will be repeated as long as new qualifications are not resolved, providing that after the deployment of the second patch, additional Charges will be imposed for any subsequent patches deployed.

Notwithstanding the above, Operational Acceptance Testing will be deemed to have taken place if there shall be no response from Customer (Deemed Acceptance) five (5) working days after Customer is notified that the qualification has been resolved.

Upon Acceptance or Deemed Acceptance, invoicing will commence for the setup Charges and usage Charges for the Management services (billed monthly in arrears).

If Customer has chosen Managed OS and does not comply with the schedule for the deployment of Customer Application jointly agreed with Orange, Orange reserves the rights to declare the acceptance of the Operational Acceptance Testing.

In any case, Orange is only committed to supply the technical solution as defined in the Low Level Design, a document which is agreed upon by both Customer and Orange. Therefore, Customer may only qualify the Operational Acceptance Testing in accordance with the provisions hereof if the solution deployed by Orange is not compliant with the Low Level Design and the deliverables supplied by Customer.

Also, if Orange detects discrepancies between the technical elements supplied by Customer in their deliverables and Customer's real technical environment, and these discrepancies generate additional costs to Orange, it may review the charges for the Service and a new Order Form must be signed by Customer before the additional services are implemented.

1.3.6 Operational Service Verification

During the Operational Service Verification phase, Customer shall approve Customer Solution in operational mode.

Customer may not refuse to approve Operational Service Verification and to sign the accompanying minutes unless there is a case of minor or major regression of the solution compared to its run validated under Operational Acceptance Testing (hereafter minor qualification or major qualification) based on the same criteria set out above for Operational Acceptance Testing.

In case of a minor or major regression, Customer shall contact Customer Support Center.

Following the Operational Service Verification:

- Customer will approve the Operational Service Verification by signing the Operational Service Verification minutes without qualification; or
- Customer would issue either minor or major acceptance qualification. Orange undertakes to resolve the qualification as soon as possible. Notwithstanding the above, Operational Service Verification will be deemed to have taken place if there shall be no response from Customer (Deemed Acceptance) after ten (10) working days following the resolution of the qualification as notified by Orange.

Orange commitments on SLA will commence only after acceptance of the Operational Service Verification approval.

Upon Acceptance or Deemed Acceptance, invoicing will commence for the following Charges:

- Usage Charges for the GTTR (billed monthly in arrears).
- Usage Charges for the Changes (billed monthly in arrears).
- Usage Charges for the Application probes, if applicable (billed monthly in arrears).

- Charges for Consulting Services,
- Any other technical tuning of Customer Application Charges, if applicable.

1.4 Service Management

1.4.1 Service Support

1.4.1.1 Customer Support Center

Customer Support Center is the primary point of contact for incident management.

Customer Support Center is available 24x7. Customer support is provided in English.

Customers can also open incident tickets through the MSCT access via the My Service Space portal.

1.4.1.2 My Service Space Portal

Orange provides Customer with access to the web portal, My Service Space, accessible through an URL, with authentication. My Service Space portal provides access to the following:

- **Flexible Computing Console:** allows Customer to view usage statistics of the Customer Platform resource pools. This portal is accessed through an URL with authentication.
- **Service dashboard:** allows Customer to view the performance and availability of Customer Platform Virtual Machines, operating systems and middleware.
- **Managed Services Changes Tool – MSCT:** allows Customer to issue technical change requests to be performed by Orange (see Clause 1.4.4 Change Management). Customer will connect to the MSCT portal using a secured link 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.
- **Service support:** This function allows Customer to open incident tickets. Customer can also open an incident ticket by calling, 24x7, Customer Support Center. The tool allows the follow-up of the processing of incident tickets, whichever the channel used to open them, and the consultation of the history of processed incident tickets.
- **Information center**: In this area, Customer will find the following documents:
  - Contract
  - Purchase Order
  - Minutes of Customer Meetings
  - Project Documents
- **Billing:** The billing function is an optional function that allows Customer to consult online and to download duplicate invoices in PDF format, together with all appendices. Customer can search, display and download their invoices over a maximum period of rolling 12 months.

1.4.1.3 Customer Service Manager

Orange provides Customer with a customer service manager who is the contact point for Customer for operational matters. The customer service manager ensures compliance with overall service quality and Customer's satisfaction.

1.4.2 Continuity Management

The services related to continuity management cover the activities that are necessary to ensure the continuity of the Service in spite of a Service disruption or programmed shutdown.

Orange proposes to each Customer a continuity management process in order to make sure that Customer Application are protected or may be restored as quickly as possible in the event of an incident.

The Service-continuity rules must nevertheless have been incorporated in the design of Customer Application. Among the deliverables expected from Customer include, for each Customer Application, the presentation of the Customer Application architecture, to ensure the management of the Service continuity.

1.4.3 Capacity Management

With regard to the sizing information supplied by Customer, the capacity management provided by Orange aims to define a Customer Platform that corresponds to Customer's business expectations in a profitable and timely manner.

Capacity management essentially consists of seeking a balance between:

- **Costs and capacity:** it is necessary to make the best use of the available resources in order to identify purchases of additional processing capacity in relation to Customer's requirements.
- **Supply and demand:** make sure that the available supplied processing power corresponds to the demand. Demand is conditioned by the activity as forecasted from the beginning until the end

of the Service and defined in the Low Level Design; it may prove necessary to make choices concerning the demand, or influence it for some resources.

1.4.4 Change Management

Change management applies following a service change request from the Customer.

The entry points for a change request are:

- For any change request described in the Change Catalog: My Service Space portal through Managed Services Changes Tool – MSCT. The list of persons authorized to submit change requests is provided by Customer to Customer Service Manager on completion of Operational Service Verification.
- Any change request made via the MSCT tool with the connection identifiers provided by Orange implies a change request made by Customer, regardless of the person who made this request on behalf of Customer.

Change requests may or may not modify the Service scope. If the requested change amounts to a new service, a new order must be placed by Customer. In any case, the submission of a change request via the MSCT tool holds for the acceptance by Customer of this change and the associated application conditions and invoicing. Therefore, Orange recommends to Customers to check the potential impact for Customer Solution, before any submission of a change request via MSCT.

Change requests are covered by Orange Guaranteed Time To Change (GTTC), as set out in the Service Level Agreement for Flexible Computing Premium.

Change requests maybe invoiced by Orange as per the Charges Schedule. Orange reserves the right to charge more than the Charges Schedule, if the nature of the change request justifies it; after agreement with Customer, and before the requested change is acted upon.

- For any other requests that are not contained in the Change Catalog, Customer shall contact the Orange sales representative, who will study the request and provide a build plan and an evaluation of the charges.

Orange may accept the requested change request as is or propose the appropriate modifications to the requested change request.

Changes planned at the initiative of Orange are dealt with in Clause 1.4.10 Management of Patches and Scheduled Tasks.

1.4.5 Incident Management

The service incorporates an incident management process. The objectives of this process are to:

- intervene in case of real or potential breakdowns of Customer Solution,
- maintain communication between Orange and Customer concerning the situation related to the incident,
- assess the incident to determine if it is likely to occur again or reveals a chronic problem.

Orange handles incidents:

- in proactive mode, following the detection of an incident by the monitoring tools,
- in reactive mode, following an incident reported by Customer via Customer Support Center.

The different steps of an incident processing (whether reported in proactive or reactive mode) are:

- acknowledgement of the report of incident,
- evaluation of the incident severity,
- analysis and diagnostic,
- resolution and operation recovery,
- closure of the incident in agreement with Customer.

1.4.6 Configuration Management

Orange manages the repositories that register the configurations of all the elements that make up the Service.

1.4.7 Release and Deployment Management

With release and deployment management, Orange deals with all updates provided by hardware and software suppliers. This includes minor updates – patches and service packs – and major updates.

Application of major updates will be charged additionally. When Orange decides to put a new component into production, the production release procedure is dealt with as a change request, in accordance with the rules defined for the Management of patches and scheduled tasks.

Orange ensures the traceability of all interventions in production via an operating tool used at all levels of Customer Support center. This data is retained by Orange for the duration of the Contract and shall be conclusive between Orange and Customer.

1.4.8 Monitoring

Orange monitors Customer Solution in two complementary ways:

- presence of Customer Solution components and their ability to respond to test check,
- check security perimeter built with Customer for Customer Application.

Incident management is based on the implementation of an automatic monitoring of Customer Platform components.

Orange implements an appropriate monitoring environment and alert management for all equipment except those excluded in the Low Level Design.

This environment can alert the Orange supervision teams in case of Customer Platform malfunctions, so that they can initiate check and corrective actions.

Two types of monitoring are implemented:

- Remote monitoring: Customer Solution is monitored and analyzed on a regular basis, as deemed necessary by Orange, based on industry best practice The result of this analysis determines whether or not a monitoring alarm shall be raised;
- Local monitoring: Orange can install software agents on its servers. This software agent regularly checks various operating-system parameters and transmits the tests results to the central monitoring solution. This translates any alarms into a standard format and sends them to the monitoring consoles.

1.4.9 Modification and Evolution Management

Orange does not manage Customer Application technical development. These developments are the responsibility of Customer, with their integrator or software publisher.

Orange manages modification and evolution to its infrastructure according to Clause 1.4.10 Management of Patches and Scheduled Tasks.

1.4.10 Management of Patches and Scheduled Tasks

Scheduled task consists of the changes planned at the initiative of Orange.

1.4.10.1 Scheduled Task on the Shared Platform

Orange reserves the right to interrupt access to the Service to carry out any preventative, routine or scheduled maintenance (collectively Planned Maintenance) with regard to the shared platform which Orange reasonably believes it is necessary in order to prevent or remedy a defect which may affect Customer's use or access to Service. To this end, Orange will have a maximum of two timeslots not exceeding 60 minutes per calendar month, to carry out Planned Maintenance.

Not all Planned Maintenance will impact the availability of a Customer's Service, but in case of interruptions to the Service, the unavailability shall be deemed as an excluded event for the purpose of calculating the Guaranteed Service Availability Rate.

Except in the event of an emergency, Orange will endeavor to provide Customer with five (5) calendar days prior email notification before implementation of the Planned Maintenance.

1.4.10.2 Scheduled Task on Customer Solution

For Planned Maintenance on Customer Solution, Orange will propose three timeslots for Customer to choose from for the maintenance to be carried out. Guideline on how Planned Maintenance will be performed is contained in the document entitled Customer Operational Guide.

The Planned Maintenance here includes the management of patches for operating systems and middleware managed by Orange, depending on the service management subscribed by Customer. On this subject, Orange undertakes to apply the patches made available by the software publishers or communities.

Critical and/or urgent security patches are highly recommended to be applied. And as maintenance of Orange environment management, it is mandatory for the components to be updated. For both these cases, the updates will commence automatically after the notice given by Orange.

It is the responsibility of Customer to check that the application of the patch does not cause any deterioration to Customer Application.

1.4.11 Version Management

Orange undertakes to manage the versions of operating systems and software that have software editor support or open-source support; as soon as the version is no longer supported by the software editor or open-source support, the commitments of Orange cease. Customer must ensure that Customer Solution is upgraded to the applicable higher supported version. Orange may, upon request from Customer, offer chargeable consulting services to accompany this upgrade.

1.5 Service Restrictions

Customer shall ensure that it takes all necessary technical precautions for the use of Service and the compatibility of their Customer Application with Service.

Due to the sharing of the Orange hosting platforms, the Customer must comply with the technical programming standards and more generally with all instructions from Orange intended to ensure the quality of service supplied to customers.

Customer also undertakes not to or cause anyone else to do any act or omission that is likely to harm the configuration of Orange' hosting platform, its security or its run, or the Flexible Computing Premium solution allocated to Customer.

Customer undertakes to comply with Service usage requirements as may be notified to them by Orange.

Orange shall not be held liable if the actual number of connections, requests, or server resources consumption exceeds Customer's forecasts.

Failure by Customer to comply with the technical restrictions hereof shall constitute a material breach of the Agreement.

1.6 Invoicing

The Customer's Charges Schedule provided to Customer indicates all the services that will be invoiced. This document is signed by Customer.

The charges of the Consulting Services as defined in the Charges Schedule will be reviewed on a yearly basis at the contract signature anniversary date and the revised charges will henceforth apply. The revised charges will then serve as basis for the billing of the referenced service, without the need for an amendment to the contract.

1.7 Security

1.7.1 Obligations of the Parties on Logs

The obligations of Parties for the collection, archiving, and retention of security logs are dependent on the Management Services selected by Customer as detailed in Table 1.

The period of retention of logs by Orange is one (1) week on line on the security server, and archived one year off line for legal request, from their creation date.

Table 1: Management Services - Obligations

Management Service	Managed OS	Middleware Monitoring	Managed Middleware	Application Outsourcing
Front End Firewall ▪ Traffic logs (timestamp). ▪ IP Source/Destination.	Orange	Orange	Orange	Orange
Gateway SSL (trace customer's operators coming from internet)	Orange	Orange	Orange	Orange
OS ▪ Customer authentication logs (timestamp). ▪ Log-in/log-out, authentication errors. ▪ IP.	Customer‡	Customer‡	Orange	Orange
Middleware	Customer	Customer	Orange	Orange
Customer Application ▪ Customer authentication logs (timestamp). ▪ Log-in/log-out, authentication errors. ▪ IP Source/Destination. ▪ Data. ▪ Creation, modification, suppression.	Customer	Customer	Customer‡	Customer‡

Key	
Orange	Responsibility of Orange.
Customer	Responsibility of Customer.
Customer‡	Responsibility of customer as a whole but, with the collection part delegated to Orange.

1.7.2 Management of Security Patches

Orange manages the major security patches on the operating systems and middleware in the Charges Schedule (see Clause 1.4.10 Management of Patches and Scheduled Tasks).

1.8 Reversibility

Reversibility refers to the ability for Customer to get back their Customer Application as well as associated Data, deployed on Customer Platform.

The ownership of the dedicated physical servers is not transferable to Customer.

Reversibility will be triggered by Customer by sending Orange a registered letter with return receipt no later than one (1) month before the expiration or termination of the Contract.

The period of reversibility will be limited to one (1) month from the date of receipt by Orange of Customer's request. Extension of the period of reversibility is subject to additional Charges. During this period, Customer will be granted the administration right on the Customer Platform.

The reversibility of Service may not be triggered in case of termination of the contract by Orange due to a fault by Customer. The reversibility will only consist of allowing Customer to recover their Data processed by Orange under the Contract. The extent of the Data recoverable is subject always to the Customer's opted backup retention period.

If additional assistance to that defined above is requested from Orange, Customer will receive:

- A proposal for paid assistance, specifying the conditions of its assistance, the personnel dedicated to the reversibility operations and any necessary hardware and physical facilities.
- The Charges applicable to providing this additional assistance.

1.9 Order Term and Termination

1.9.1 Duration of Orders

Each Order takes effect from signature of the Order form by Customer.

Each Order for Service or an optional service, as opted by the Customer, will have a Service Term of 3 months, 1 year, or 3 years from the date of Operational Acceptance Testing.

Except in the case of written notice of termination by Customer, sent to Orange by registered letter with return receipt, each Order for Service or for an optional service shall be automatically renewed for a period corresponding to the initial subscribed duration. This notice of termination must take place at least 3 months before expiration for Orders of 1 year and 3 years, and 1 month before expiration for Orders of a period of 3 months.

Notwithstanding the above, each Order for Service for dedicated physical servers is subscribed for an indeterminate period associated with a minimum period of 12 months from the date of Operational Acceptance Testing.

Likewise, certain licenses are subscribed for an indeterminate period associated with a minimum period specified in the Order form, starting from the Date of Technical Acceptance Test.

In case the Order form is sent by fax or scanned via email, Orange must receive the original Order form by post, dated, initialed, and signed by Customer no later than one month after reception by Orange of the Order form sent by fax. Orange' proposal expires after this period.

1.9.2 Termination of Orders

Customer may terminate the Service or an optional service at their discretion, by registered letter with return receipt, giving notice of three months for Orders of 1 year and 3 years, and one month for Orders of a period of 3 months.

In case of termination by Customer of an Order without cause before the Operational Acceptance Test, the full Charges under Clause 1.3.3 incurred up until the termination date shall be payable by Customer.

In case of termination of the Order for Service or an optional service by Customer without cause after the Operational Acceptance Testing and before the end of the Service Term, Customer is liable for a penalty equal to the total Charges for the remaining Service Term. For the purpose of calculating the total usage Charges for the remaining Service Term, the Charges shall be based on the average total spending for the past months up until the termination date. If the termination is prior to the completion of a full usage month, then the usage Charges shall be the estimate usage based on the Customer's server consumption resources forecast.

1.10 Geographic Availability

The Service is available worldwide. The Customer Solution will be located in a data centers of Orange located in France or in Singapore according to the choice of Customer as defined in the Order form of the Service.

END OF SERVICE DESCRIPTION FOR FLEXIBLE COMPUTING PREMIUM SERVICE