1 SERVICE DESCRIPTION FOR DEVICE MANAGEMENT PREMIUM

1.1 Definitions

All capitalized terms used but not defined herein will have the meanings given to such terms elsewhere in the Agreement. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions in this Service Description will control for purposes of this Service Description.

"**BYOD**" or "**Bring Your Own Device**" means the policy of permitting employees to bring personally owned mobile devices to their workplace.

"**Client Software**" means the software which allows the Device to connect to the Device Management Software that is provided by Orange and installed on each Device.

"**Device**" means the Smartphone or Tablet unit, which the Service allows Customer to manage.

"**Device Management Software**" means the MobileIron server for Device management.

"**EULA**" means End User License Agreement.

"**End-User Portal**" means a web site, part of the Device Management Software, aimed at providing Users means to enroll and wipe their device(s) on their own.

"**Incident**" means a fault, failure, or malfunction in the Service. Incidents do not include Service unavailability during Scheduled Maintenance.

"**IT Manager**": A person, within Customer, identified; (i) as the single point of contact for Orange regarding the Service and/or (ii) as the person who will connect to the Management Console (recipient of login access) as well as MSCT.

"**Management Console**" means the console to which the IT Manager may connect via the Internet to manage its Service. Except as otherwise expressly agreed upon by the Parties in writing, all information provided and made available on the Management Console will be in English only. Orange will provide (and may change from time to time) the URL, login and/or password for access to the Management Console.

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

"**Operating System**" means the software installed on the Device, which manages the Device resources.

"**Reverse-proxy**" means a server placed between a client and a server. Incoming requests are handled by the reverse- proxy, which interacts on behalf of the client with the desired server or service residing on the server.

"**Scheduled Maintenance**" means routine maintenance scheduled by Orange to implement generic changes to, or updates of, the Orange Services or the Orange Network.

"**Service**" means the Device management service provided by Orange as set out in this Service Description.

"**Service Request Form**" or "**SRF**" means the form that details the Customer's specific Service requirements.

"**Smartphone**" means a mobile phone that also works as a small computer that allows Users to exchange email as well as run mobile applications or applications.

"**Tablet**" means a mobile computer, larger than a mobile phone, integrated into a flat touch screen unit that uses a stylus, digital pen, or fingertip as the primary input device.

"**User**" means Users of the Service who have been authorized by Customer. Users use the Service under the responsibility of the Customer.

"**VPN**": Virtual Private Network.

1.2 Description of the Service

The Service includes the Device Management Software, Client Software, and associated services. The Service provides Customer with a single Management Console to centrally manage and secure Devices and deploy mobile applications as well as with an End-User portal so that a User can perform basic administrative tasks without contacting the IT department, such as registering a new device or wiping a device he would have lost.

Device Management Software and associated services allow Customer to inventory, set, and update configuration, and security policies, distribute mobile applications, control access to corporate resources to compliant devices only, and troubleshoot devices remotely over-the-air.

Security features are intended to protect corporate information from unwarranted settings and data access, either directly on the Device or by remotely hacking the Device. They also allow enabling the system encryption as well as remote lock-and-wipe of devices.

The Device Management Software is hosted by Orange and is operated on a 24 hours a day, 7 days a week basis by Orange as a managed service.

1.3 Service Request Form

1.3.1 **Customer Requirements:** Prior to commencement of the Service, Customer and Orange will complete a Service Request Form. Customer will provide all relevant technical specifications and documentation regarding its policies for mobile Devices (passcode, restrictions, WIFI, VPN, applications, etc.) and Orange will reasonably assist Customer in completion of the SRF. Customer will ensure that all information contained in the completed SRFs is accurate.

1.3.2 **Customer Contacts:** Customer will identify a primary contact and a secondary contact in each SRF. Customer will ensure that the primary and secondary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week. Orange will respond only to the Service requests and calls regarding Incidents issued by such contacts. All communications between the Orange and Customer will be in English, unless otherwise agreed to by the Parties.

For Severity Level 1 and Severity Level 2 Incidents, Orange will notify Customer's security contacts of the Incident using all contact details provided in the SRF. For Severity Level 3 Incidents, Orange will send a message to the email addresses set out in the SRF.

The primary contact identified in the SRF will ensure that:

- All contact information is maintained and is current;
- Orange is notified before and after any planned outages or configuration changes to Customer's network or network services; and
- All configuration changes are scheduled at least 5 Business Days in advance.

All changes to Customer's primary contact must be made in writing, on Customer's letterhead, and be signed by a senior manager in Customer's organization.

1.4 Service Deployment

1.4.1 **Lead Time Requirements:** The time to deploy the Service is measured only when Orange has received both a signed Order and a fully completed SRF. The time to deploy the Service is 4 weeks as of receipt by Orange of the two documents. The deployment will be delayed if Customer does not provide both documents or if the Customer requires changes to the specifications listed in the completed and accepted SRF.

1.4.2 **Configuration:** Orange will configure the Device Management Software exclusively based upon specifications contained in the applicable SRF. Any configuration changes required due to inaccurate or revised specifications will be charged to and paid by Customer at the Hourly Labor Rate for such services, plus Expenses.

1.4.3 **MDM Platform Change:** Following service opening, Orange will accept requests for changes to the configuration of the Device Management Software only from the security contacts identified in the SRF. All such changes will have to be requested through MSCT.

1.4.4 **Server Upgrades:** Orange will provide version management of the Device Management Software and of the Client Software; provided, however, that nothing contained herein will require Orange to provide all new releases of Software. Orange, in its sole discretion, will decide when upgrades take place. If Orange needs to take a Device or all or part of the Service off-line to implement Software updates or network enhancements, Orange will provide at least 7 days prior written notice of such events. When possible, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement Software or Service upgrades remotely during Business Hours.

1.4.5 **Acceptance Testing:** Upon completion of the installation of the Device Management Software, Orange will commence its own acceptance testing, which will confirm that all aspects of the Service are operational in accordance with the terms of this Service Description and the parameters set forth in the SRF. Upon completion of this internal acceptance testing, Orange will send to the security contacts listed in the SRF a "**Welcome mail**" confirming that the Service is ready to be used and is operational.

1.4.6 **Security Policy Changes Procedure:** Following installation and acceptance testing, Orange will accept requests for changes to the Device Management Software only from the security contacts identified in the SRF. All such changes will have to be requested through MSCT. If Orange requires additional information to finalize the implementation of the change, Orange reserves the right to contact the primary security contact to agree to the appropriate actions, timeframes, and charges, if applicable.

1.5 Service Features

Device Management Premium comes with two different packs; standard pack and advanced pack. Features available with each pack are listed hereafter.

1.5.1 Standard Pack

(a) **Device Inventory:** The Device Management Software allows centralized scanning and capturing of hardware and software asset information from the Devices. Captured asset information is available on the Management Console.

(b) **Configuration and Security Policies:** With the Service, the Customer is able to remotely configure and maintain Device settings. This allows management control of Devices' behavior and of the availability of certain features and default settings of the Devices for User experience, security, and policy enforcement purposes. The set of configurable settings and policies depends on Devices' manufacturer and Operating System version.

(i) The Service enables the Customer to centrally and remotely enforce password, on Device encryption, and apply restrictions or other security features such as jailbreak and root detection.

(ii) The Service allows the ability to remotely lock and wipe Devices should they be lost or stolen.

(c) **Compliance Policies:** The service allows monitoring of Devices for compliance and automatically enforces compliance action when a Device falls out of compliance. Automatic remediation actions include notifying the User, blocking access to the enterprise from the Device, or quarantining the Device.

(d) **Management of Mobile Application:** The Service provides a built-in enterprise application store to distribute mobile applications to Users provides an application inventory that presents a snapshot of the applications installed across all employees' managed Devices and provides application control to enforce corporate application policy based on required, allowed, and disallowed applications.

(e) **Roaming Control:** The Service can remotely set roaming controls. Depending on the manufacturer of the Devise and OS version, data and/or voice could be disabled while roaming.

(f) **Enterprise integration:** The Service provides a deep Integration with Customer AD/LDAP groups and attributes to authenticate Users connecting the End-User Portal, to automate Device configuration and to assign policies based on group membership.

(g) **BYOD Support:** The Service supports both corporate-liable and individual-liable Devices.

1.5.2 Advanced Pack:

The advanced pack includes all the features of Standard pack plus the following:

(a) **Secure Application Container:** Customer can create a secure application container. This container is connected to other secure app containers and to the Management Console for ongoing management. Security features provided by the secure app container include data-at-rest encryption, single sign-on, data loss prevention, open-in controls, dynamic configuration, and selective wipe of app-specific data. All application containers are integrated with the Device Management Software for policy management.

(b) **Secure Browser:** The Service includes a secure browser to provide a VPN-less access to internal websites and web applications, while preserving a native and high-fidelity web browsing experience. It requires the use of a reverse-proxy that is part of the Service.

(c) **Secure Access to SharePoint Sites:** The Service provides VPN-less access, storage, and viewing of documents from corporate SharePoint sites and allows the administrator to establish data loss prevention controls to protect these documents from unauthorized distribution. Users have seamless connectivity to enterprise resources behind the firewall. It requires the use of a reverse-proxy that is part of the Service.

(d) **Secure Mail Client for Android:** The Service provides a secure mail client that works for all Devices running Android operating system (as from Android version 4.0) and preserve native experience. It leverages the secure application container to secure email data both in motion and at rest on the Device. All email content, including attachments, is encrypted and stored in a secure container.

1.6 Changes by the Customer

All platform changes are managed by Orange. Those changes include integration features such as email access control setup, integration with customer Active Directory. Whenever those changes have an impact on pricing (e.g. new proxy-server, use of advanced pack if not already in pricing agreement), an Order will first be required.

The IT Manager will be fully responsible to implement, manage and change "**Configurations & Policies**", "**Application**" as well as "**Logs & Events**" settings, from the Management Console, in

accordance with Customer corporate IT and HR policies. All operations on Devices (e.g. lock/unlock, retire/wipe, localize, block) as well as end-user support are also the responsibility of the Customer.

All these changes are realized by the IT Manager himself as Orange shall not be liable for any consequence of these changes.

1.7 Optional Features

Optional features are available with both standard and advanced packs.

1.7.1 **Email Access Control Option:** Email Access Control is an optional feature that allows the Customer to secure the access from Devices to the corporate email servers. This option can be used to ensure that only Devices that comply with corporate policies can access mail server(s). This option works with a reverse-proxy.

1.7.2 **Certificate Distribution:** After the interconnection with Customer Certificate Authority, the Service can distribute identity certificate to managed Devices for authenticating User when launching corporate email, WIFI, VPN or secure application. The Service acts as a relay which prevents Customer from publishing internal Certificate Authority on the Internet.

While enrolling a Device, or when new configuration or new application is pushed to a Device, the User may have to accept the EULA from the mobile vendor (e.g. Apple or Samsung), or accept the EULA for mobile application or settings pushed by the Service but not part of it (e.g. MS ActiveSync). Refusing those EULA will prevent service/feature activation.

1.7.3 **Service Manager:** As for other Orange services, the Service Manager is the Customer's primary point of contact within Orange. The Service Manager provides Customer with a monthly dashboard and reporting analysis and is responsible for the verification of the Service performance. SLA for the Service will only apply if the Customer has ordered a Service Manager.

1.8 Maintenance of the Service

1.8.1 **Remedial Maintenance:** Orange will maintain the Service in Proper Operational Condition. If a Fault is caused by a failure in any Service component, Orange will repair the Fault following receipt of a Fault Call or upon detection of the Incident by Orange, whichever occurs first.

The GCSC will classify all Fault Calls and Incidents as follows:

Severity 1	Problems causing critical impact to the business function(s) or customer(s). Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible.
Severity 2	Problems causing degradation of service resulting in impact to business function of customer. Impact justifies priority attention and application of resources to resolve in a timely manner.
Severity 3	Problems causing low impact to the business function(s) and customer(s). Requires timely resolution to minimize future impacts. Resources should be allocated in accordance with normal managerial planning prioritization.

1.8.2 **Remedial Maintenance Exclusions:** Orange will have no obligation to provide remedial maintenance services for, nor will Orange be liable to Customer for damages for loss of the Service or the Device Management Software caused by any of the following (collectively "**Limitations**"):

(a) Damage to the management infrastructure caused by any Force Majeure Event, or any other casualty or loss;

(b) Any instability in the operation of the Device Management Software that is caused by or is related to the use of certain software, or by any other software provided by Customer or its designees, or by combination of the Device Management Software with other software, even if such combination is specified on a duly accepted SRF; and/or

(c) Fault calls and Remedial Maintenance services rendered necessary by the above causes may be performed by Orange at Customer's request, and will be charged to and paid by Customer at the Hourly Labor Rate, plus Expenses.

In addition, the Service excludes:

(a) Maintenance of Devices not specified in the SRFs; and/or

(b) Correction of software databases and/or programming errors or any errors or damages caused by or arising out of input or error, except as otherwise set forth in this Service Description.

1.9 Licensing Terms

1.9.1 Orange grants to Customer and its Users, for the Service Term of the applicable Order, non-exclusive and non-transferable licenses to use the Client Software and the Device Management Software, in object form only, strictly for purposes of using the Service. Customer will not produce, copy (except for the purpose of retaining a back-up copy), alter, modify, or add to the Client Software or the Device Management Software or any part thereof, or attempt or allow a third party to attempt to reverse

engineer, translate or convert such Software from machine readable to human readable form, except as permitted by applicable law. Customer will not sell, assign, license, sublicense or otherwise transfer, transmit or convey the Client Software or the Device Management Software, or any copies or modifications thereof, or any interest therein, to any third party. Customer will not use the Client Software or the Device Management Software:

(a) in connection with the products or services of any third party; or

(b) to provide services for the benefit of any third party. In addition, use of the Client Software and the Device Management Software is subject to the applicable manufacturer's software license agreement.

1.9.2 Orange is solely responsible for the provision of the Services, Customer Software, and the Device Management Software hereunder, and Customer will have no right, claim, or cause of action against the subcontractors of Orange or licensors.

1.10 Pricing

One-time and monthly recurring Charges apply.

1.10.1 **One-time Charge:** The One-Time Charge includes the Service setup cost and a fixed Charge for each Device ordered, the amount of which varies according to the number of signed Devices as well as the selected optional features.

1.10.2 **Monthly Recurring Charges:** A monthly recurring Charge applies per Device using the Service in any month, which amount varies according to the number of committed Devices as well as the optional features.

If, in any month, the actual amount of monthly recurring Charges is less than the total amount of fixed Charges for all Devices initially ordered, Orange will invoice Customer for such month an amount equal to the total amount of fixed Charges for all Devices initially ordered.

If, in any month, the actual amount of monthly recurring Charges is more than the total amount of fixed Charges for all Devices initially ordered, Orange will invoice Customer for such month an amount equal to the actual amount of monthly recurring Charges.

The comparison between the actual amount of monthly recurring Charges and the total amount of fixed Charges for all Devices initially ordered will be done on the basis of monthly reports extracted from the Device Management Software.

1.11 Order Term and Termination

1.11.1 **Term and Termination:** Each Order will have a Service Term of 36 months following the Date of Acceptance of the Service, and will be automatically renewed for successive Extended Terms of 12 months, unless terminated earlier pursuant to the General Conditions.

1.11.2 **Termination for Convenience**

(a) **Termination of the Order:** Customer will be entitled to terminate an Order at any time for convenience, subject to the payment of early termination fees. 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 the Service Term or Extended Term, as applicable had no termination occurred.

(b) **Cancellation of Optional Components:** Customer will be entitled to cancel each optional component by providing Orange at least 90 days' notice prior to the end of the Service Term or Extended Term as applicable. Otherwise optional components will be automatically extended for successive Extended Terms.

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 been due until the end of the then current Service Term or Extended Term.

1.11.3 **Conditions of Termination:** Upon receipt of the notice of termination, Orange will acknowledge the termination by mail to the IT Manager. 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 Management Console. 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 appropriate contact listed in the SRF.

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

1.12 General Availability and Limitations of the Service

The Service is not available for all Device types. Supported Devices includes Devices with the Operating System versions listed in the table below. Orange may remove from or add to such list from time to time, without liability to the Customer.

Operating System	Supported Versions
Apple iOS	iOS 4.O and later
Google Android	version 2.3 and later
Windows Phone	Windows Phone 8

In order for the Service to work, Devices must be powered on and always have Internet connectivity to the Device Management Software, either via mobile data or WIFI.

The available features and functions vary depending on the Device's Operating System that is used. Some of the features require monitoring of Devices, changing settings on Devices and installing software. This needs to be endorsed by the Customer.

While using the Service, the Customer, and each of its individual Users, must not engage in conduct which is unlawful, fraudulent, or negligent. Customer is responsible for the conduct of its nominated person(s) and Users that use the Management Console.

Device manufacturers may, over time, restate or amend the terms and conditions applicable to the relevant Device. The Service is subject to those terms and conditions and conditional upon the Customer accepting any such Device related terms and conditions.

1.13 Geographical and Legal Service Availability

Some features of the Service are based on SSL/TLS standards. Encryption of the Device or part of the Device can also be activated. This Service is thus embedding or using cryptographic software. Depending on the country, the Users will connect from, the use or import of such materials may be subject to specific conditions. The Customer will verify whether it is, and their Users, are legally allowed to use the Service in the countries where Users use the Service.

END OF SERVICE DESCRIPTION FOR DEVICE MANAGEMENT PREMIUM