1 SERVICE DESCRIPTION FOR SECURE MY DEVICE

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.

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

"**Anti-Virus Software**" means the Software provided by Orange as part of the Secure My Device Service that screens incoming data for potentially malicious software codes.

"**Device**" means the User laptop, desktop, PDA, or Customer server for which Orange provides the Secure My Device Service.

"**Incident**" means a fault, failure, or malfunction in the Secure My Device Service.

"**Personal Firewall**" means the Software installed and administered on a Device to enhance security for that Device.

"**IT Manager Guide**" means the Information Technology Manager guide provided by Orange, which identifies the standard Security Profiles, validated security rules, and usage conditions for the Secure My Device Service.

"**Security Policy**" means an ordered set of rules configured in the Administration Console and against which a Device's connection is checked. The Security Policies filter and authorize the acceptance or rejection of traffic based on specified criteria, which may include the source, destination, protocol, port or application of the traffic.

"**Security Profile**" means the set of Security Policies that applies to a group of Users.

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

"**SMD Software**" means the Software provided by Orange as part of the Secure My Device Service that Customer will install on the Devices and that allows Customer to manage such Devices and the Security Policy through the Administration Console.

1.2 SRF and Security Policies

1.2.1 Customer SRF Requirements

Prior to commencement of the Secure My Device Service, the Parties will complete the applicable SRFs. Customer will provide all technical specifications and documentation regarding its existing network, and Orange will reasonably assist Customer in completing the SRFs; however, Customer will ensure that all information contained in the completed SRFs is accurate.

1.2.2 Customer Security Contacts

Customer will identify a primary security contact and between 1 and 3 secondary security contacts in each SRF. Customer will ensure that all primary and secondary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week. All Incidents will be reported to the listed contacts, and Orange will respond only to Service requests and calls regarding Incidents issued by such contacts.

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 forth in the SRF. All contacts by Orange will be made in English, unless otherwise agreed to by the Parties.

The primary security contact identified in the SRF will ensure that:

- All security contact information is maintained and 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 security contact must be made in writing, on Customer's letterhead, and signed by a senior manager in Customer's organization.

1.3 Description of Services

The Secure My Device Service is a fully managed Security Service that includes the Administration Console and SMD Software. Customer must provide and define a Device that meets the Orange requirements for, and that will serve as, Customer's primary Secure My Device relay agent, and Customer will configure and use such Device in accordance with the instructions from Orange. Customer will install the SMD Software and all upgrades thereto provided by Orange on each Device, including the Device acting as Customer's primary relay agent; Orange will determine in its sole discretion which releases of and upgrades to the SMD Software to make available for the Service. Upon installation, the SMD Software will connect the Device to the Administration Console and regularly update the Security Policies to the Device from the Administration Console. If Orange provides an upgrade of the SMD Software, Orange will provide such upgrade on the Administration Console, and the User can accept the upgrade immediately or postpone the upgrade the next time the Device connects to the Administration Console. Using the Administration Console, Customer will select the service options that it will receive as part of the Secure My Device Service, and those service options (as described more fully below) include the following: Compliance and Patch Management; Security Software Continuous Compliance; Anti-Virus/Anti-Spyware; Personal Firewall; Comply, Enforce and Remediate; Business Everywhere Connection Client Update; and Application Patch Management services.

1.3.1 Service Requirements

Customer must provide Internet access authorizing the Service data flows (e.g. Customer will ensure that its firewall or proxy configurations comply) for use with the Secure My Device Service, and Orange will identify, and may modify from time to time, the operating systems that can be used with the Secure My Device Service. Orange also will identify, and may modify from time to time, the third-party firewall, anti-virus and Spyware tools, and services that Customer may use with the Secure My Device Service. Except as otherwise expressly provided in this Agreement, Customer will obtain and maintain all licenses necessary to use the operating system, firewall, anti-virus and Spyware tools and services with the Secure My Device Service.

1.3.2 Compliance and Patch Management

Subject to Clause 1.3.1 above, Orange will provide patches and updates to Customer's operating system through the Administration Console, which Customer may manage, download, and install on the Devices. The Administration Console also will identify select top vulnerabilities on the Devices, for which Customer may elect to take corrective action. However, Orange makes no representations or warranties regarding the patches or vulnerabilities provided by or through any such updates.

1.3.3 Security Software Continuous Compliance

Customer may install Client Managers on the Devices for the supervision of the firewall, anti-virus, or Spyware services on such Devices. The Client Managers do not provide any firewall, anti-virus, or Spyware software, but subject to Clause 1.3.1 above, will allow Customer to monitor and manage such services on the Devices.

1.3.4 Anti-Virus/Anti-Spyware

Customer may receive Anti-Virus/Anti-Spyware Software as part of the Secure My Device Service. Customer may download and install on the Devices updates to the Anti-Virus/Anti-Spyware Software provided through the Administration Console. However, Orange makes no representations or warranties regarding any such updates that may be so provided.

1.3.5 Personal Firewall

Customer may receive the Personal Firewall, which will monitor and analyze the Device's incoming and outgoing communications to prevent intrusions and provides security for the Device in accordance with the Security Policies.

Orange monitors the Administration Console for the Personal Firewall presence 24 hours a day, 7 days a week. However, Orange does not monitor individual Devices. Also, monitoring of the Personal Firewall on the Administration Console does not include monitoring of operational problems relating to Customer's Internet service, web browsers, or Customer's line to the Internet.

1.3.6 Comply, Enforce and Remediate

If Customer receives the Anti-Virus/Anti-Spyware Software and Personal Firewall, then Customer also may elect to receive the Comply, Enforce and Remediate option, which automatically checks the Software provided for the Anti-Virus/Anti-Spyware and Personal Firewall to determine if such Software is running and up-to-date. If it is determined that any such Software is not running or up-to-date, then the SMD Software will attempt to launch the Anti-Virus/Anti-Spyware Software or Personal Firewall, as applicable, or the relevant update while instructing the Personal Firewall to restrict traffic to updates only. Customer may configure this option per Device, per type of Device or per group of Devices.

1.3.7 **Business Everywhere Connection Client Update**

If Customer receives the Business Everywhere Service from Orange, then Customer may elect to receive updates to the Business Everywhere Service Connection Client through the Administration Console.

1.3.8 **Application Patch Management**

Subject to Clause 1.3.1 above, Customer may download and install on the Devices important and critical updates for certain applications (as Orange will identify and may modify from time to time) made available on the Administration Console. However, Orange makes no representations or warranties regarding the patches or vulnerabilities provided by or through any such updates.

1.3.9 **Security Profiles**

Except as otherwise agreed upon by the Parties in writing, Customer will assign each User to one of the following Security Profiles:

(a) **Intranet:** All outgoing communications from the Device use a VPN tunnel, including the User's access to Customer's intranet and access to the Internet. The Intranet Security Profile cannot be used with WiFi solutions, except as expressly approved by Orange.

(b) **Internet:** All outgoing communications from the Device use a VPN tunnel, including the User's access to Customer's intranet and access to the Internet; however, if the VPN tunnel is unavailable, then the User may access the Internet directly through the Internet connectivity provided by Customer.

(c) **Customized:** Orange will customize the Security Profile for Customer using validated security rules (as described in the IT Manager Guide).

Three Security Policies are pre-defined for the Intranet Profile and the Internet Profile, one Security Policy per location or usage.

1.3.10 **Security Policies Change Procedure**

Following installation and acceptance of the Secure My Device Service, Customer will submit all changes to the Security Policies using the Administration Console, unless otherwise required or agreed to by Orange. All Security Policy changes are determined by Customer in its sole discretion, subject to any Service limitations or requirements identified by Orange, and Orange will have no liability or responsibility with respect to such changes. Customer will ensure that its security contacts will be available if needed by Orange with respect to Customer's requested changes; Customer's security contacts also will be available for any testing that may need to be performed with respect to such changes. Any potential conflict in the Security Policies or any inadvertent reduction in the security effectiveness perceived by Orange will be brought to Customer’s attention, and Orange may recommend alternative strategies.

Customer will provide all information reasonably requested by Orange with respect to any change to the Security Policies, including:

(a) Completed change on the Administration Console;

(b) Supporting details relevant to the specific change action; and

(c) Contingency plans and contact details of Customer personnel performing acceptance testing for changes to the Security Policies.

The changes will be applied to the relevant Security Policy in accordance with the IT Manager Guide, unless Customer requests Orange to apply the changes otherwise (i.e. immediately or only after Customer accepts and requests deployment of the changes); any changes or updates made to the Security Policies will be automatically downloaded to the Devices when they connect to the System.

1.3.11 **Auto-Location Feature**

The Personal Firewall can provide an auto-location feature (subject to the conditions provided in the IT Manager Guide or as otherwise described by Orange) that automatically detects the location or usage of the Device as:

(a) Locally connected to Customer's intranet;

(b) Remotely connected to Customer's intranet through the VPN tunnel; or

(c) Disconnected from Customer's intranet. The auto-location feature allows the Secure My Device Service to switch from one Security Policy to another based on the location or usage of the Device.

However, if Customer chooses a manual location instead of the auto-location, then the User must select the location and Security Policy that apply to the Device. To receive the Auto-Location Feature, Customer must:

(d) Provide the DNS or DHCP servers for the feature;

(e) Provide all information requested by Orange to allow Orange to provide the feature, and

(f) Configure its network and servers pursuant to the instructions from Orange.

1.3.12 **Service Support**

The GCSC will classify and address all 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.

Notwithstanding anything to the contrary contained in this Agreement, Orange will not provide any support directly to and will not take or respond to any calls from a User. Orange also will not provide support for the Devices or any services or software not provided by Orange.

1.4 Acceptance Testing

Customer will be deemed to have accepted, and billing will commence for, the Secure My Device Service as of the date on which Customer downloads and installs the Secure My Device Service on the Device, unless Customer notifies Orange in writing of a material fault in the Secure My Device Service for such Device within 5 Business Days of the download. In such event, the Parties will work together in good faith to correct the material fault.

1.5 Reporting

Orange will provide, and Customer may access, various reports regarding the Secure My Device Service through the Administration Console.

1.6 Charges and Service Term

Charges for the Secure My Device Service include a one-time Charge, a monthly recurring Charge per Device, and a monthly Charge based on the actual Secure My Device Service options used per Device during that month. Notwithstanding anything to the contrary contained in the Agreement, the Service Term of any Order for Secure My Device will be a minimum of 36 months.

END OF SERVICE DESCRIPTION FOR SECURE MY DEVICE