PUBLICATION 1 SERVICE DESCRIPTION FOR WEB PROTECTION SUITE

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.

"**Administrator**" means the individual(s) responsible for the administration and monitoring of Customer's security, web usage, and related policies with regard to the Web Protection Suite Services. The Administrator(s) will be identified in the SFR(s), as provided in Clause 1.2.2 below.

"**Connector Software**" means the optional software made available by Orange to Customer to allow for deployment in Customer's IT Infrastructure as described in Clause 1.4.3.2 of this Service Description.

"**End User**" means the end user of the Services described in this Service Description, which may include entities, employees, contractors and any third parties the Customer allows to use such Services. For the avoidance of doubt, all "**Users**" (as defined in the Agreement) shall also be considered End Users for purposes of this Service Description.

"**GCSC**" means the Orange Global Customer Support Centers.

"**Incident**" means a fault, failure, or malfunction in the WPS Services as reported by Customer or a security event, alert or problem with the Web Protection Suite Services

"**Internet User**" shall mean an End User of the Services who is accessing the Internet, as further described in Clause 1.4 of this Service Description.

"**IT Infrastructure**" means Customer's information technology (IT) and/or network elements (e.g. LAN, proxies, etc.) used to provision access for End Users.

"**Portal**" means the 'self-service' ScanCenter web portal that may be accessed by Administrator(s) and/or Super Users for the administration of the Web Protection Suite Services.

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

"**Super User(s)**" means the Administrator(s) or any group of individual(s) named by Customer as having responsibility for and authority to ensure compliance with Customer's security policy with respect to the Web Protection Suite Services.

"**URL**" means Uniform Resource Locator, which is the address that defines the route to a file on the World Wide Web or any other Internet facility.

"**Web Protection Suite Services**" or "**WPS Services**" means the web-related security services as described herein.

"**WPS Towers**" means the shared infrastructure platform used to deliver the WPS Services.

1.2 Service Obligations

1.2.1 **Customer Requirements.** Prior to commencement of the ordered WPS Services, the Parties will complete the applicable SRF(s). Customer will provide Orange all relevant technical specifications and documentation regarding its existing IT Infrastructure and will ensure that all information contained in the SRF(s) is accurate.

1.2.2 **Customer Security Contacts.** In each SRF, Customer will identify a primary security contact, who shall be designated as an Administrator. In addition, Customer will identify between 2 and 4 secondary security contacts, who shall also be designated as Administrators and who may grouped together as a Super User group. Customer will ensure that all Administrators serving as primary and secondary security contacts are available and can be contacted by Orange as agreed in the SRF. All Incidents will be reported to the Administrators, and Orange will respond only to Incidents and/or support requests issued by Administrators to the GCSC or via the Portal.

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

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

- All security contact information is maintained and current; and
- Orange is notified before and after any planned outages or configuration changes to Customer's IT Infrastructure or network-related services.

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 organization.

1.2.3 **Acceptable Use Policies.** Customer is solely responsible for its activities in using the WPS Services, including the activities of the End Users' and Users' adherence to Customer's Acceptable Use Policy and the Orange Policy.

Customer is responsible for ensuring that all End Users are aware of any Customer Acceptable Use Policy, as well as the Orange Policy, and for ensuring that End Users comply with these policies at all times. Customer shall defend, hold harmless and indemnify Orange against any and all liability for any violation of Customer's Acceptable Use Policy or the Orange Policy by any End User. End Users must not under any circumstances whatsoever commit, or attempt to commit, nor aid or abet any action that may threaten the Services, whether deliberately, negligently or innocently.

Customer shall notify Orange immediately upon learning of any End User's non-compliance with the Orange Policy or with Customer's Acceptable Use Policy.

1.2.4 **Software.** Customer hereby authorizes Orange to enter into the license agreements on behalf of Customer for any third party Software that forms part of the WPS Services. Such license agreements shall be based on the standard license terms of the Software vendor(s). Customer will grant to Orange for the applicable Service Term(s), a royalty-free, non-exclusive, non-transferable, revocable license to such Customer-licensed Software solely for the purpose of provisioning the WPS Services to Customer.

1.3 Scope of Services and Activation

1.3.1 Service Activation and Supply

1.3.1.1 Orange will work with Customer to determine the appropriate technical integration and set-up of the WPS Services, as well as integration with Customer's IT Infrastructure. Orange may provide Customer with a project plan outlining steps and activities relating to the provisioning of the WPS Services as part of a larger project or program, or Orange may provide Customer's technical contact and/or Administrator(s) an email explaining the necessary technical changes Customer will need to make in order to use the Web Protection Suite Services. If Customer has ordered Connector Software (as described in Clause 1.4.3.2 below), Orange will provide the relevant Connector Software (for download) to Customer, together with installation instructions. Where the Connector Software is installed on a Customer-owned server, Customer shall be responsible for the hardware, software, and licensing with respect to the Connector Software.

If Customer does not order Connector Software, then Customer will be responsible for configuring its IT Infrastructure to route all the Internet traffic to the WPS Towers.

1.3.1.2 Customer will supply Orange with all technical data and all other information Orange may reasonably request to allow Orange to supply the WPS Services to Customer. The WPS Services do not include any Internet access connection(s) or any equipment necessary for Customer to make such connection. Any Internet access service provided by Orange to Customer will be described in a separate Service Description, which will be added to this Agreement and will be subject to additional Charges.

1.3.2 Service Developments

1.3.2.1 Orange reserves the right to modify and update the features and functionality of the Services. These updates may include any subsequent release or version of the Services containing functional enhancements, extensions, error corrections, or fixes. Updates will not automatically include any release, option, or future product which maybe sold separately or which is not included under the applicable level of support.

1.3.2.2 Where practicable, Orange will give Customer prior written notice of any material modification or update, and will seek to ensure that any modifications or updates do not materially degrade the performance of the Services or Customer's use of the Services or require Customer to incur any additional cost to continue its use of the Services. Orange will use reasonable efforts to implement all such modifications or updates in a manner that minimizes the impact on the use of the Services.

1.3.2.3 Wherever possible, planned maintenance of Web Protection Suite Services is carried out on weekends or between 8 p.m. and 8 a.m. on weekdays.

1.3.3 **Acceptance Testing.** Upon completion of the installation of the Software and equipment necessary to operate the Web Protection Suite Services, Orange will commence the Acceptance Tests, which will confirm that all aspects of the Web Protection Suite Service are operational in accordance with the terms set forth in this Service Description and the parameters set forth in the SRF. Upon completion of the Acceptance Tests, Orange will provide Customer a "**Service Acceptance Form**" for Customer's execution, which form will identify the Acceptance Tests performed by Orange. Customer will be deemed to have accepted the Web Protection Suite Service on the date on which Orange issues the Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Web Protection Suite Service within 5 Business Days of receipt of the Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.4 Description of Services

The Web Protection Suite Services include the Web Malware Scanning and Web Filtering Services described below. Customer also may elect to receive the Instant Messaging Control service, Connector Software, and/or Secure Web Anywhere service as optional features and services, subject to additional Charges. Any Orders for the Web Protection Suite Service shall, at a minimum, set out the specific WPS Services (including any optional features or services) to be provided, the number of End Users, and the applicable Charges.

The End User's external HTTP, HTTPS, and FTP over HTTP requests (including all attachments, macros, or executables) are directed through the Web Protection Suite Services. The configuration settings required to direct this external traffic via the WPS Services are made and maintained by Customer's nominated technical expert and/or Administrator(s) (with assistance and support from Orange as reasonably required) and are dependent on the Customer's technical IT Infrastructure. Customer will ensure that internal HTTP/HTTPS/FTP over HTTP traffic (e.g. to the corporate intranet) is not directed to the Web Protection Suite Services.

1.4.1 **Web Malware Scanning.** Once the relevant configuration changes are made to the IT Infrastructure and the Customer web traffic is routed to the Web Protection Suite Services, unencrypted web pages and attachments will be scanned by a shared security platform that detects malware threats by using a combination of multiple, correlated detection technologies. This process is called Web Malware Scanning ("**MS**").

It may not be possible to scan certain web pages or attachments. Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through Malware Scanning unscanned.

If an End User's requested web page or attachments are found to contain malware (or is deemed unscannable, with the exception of SSL traffic), then access to that web page or attachment is denied, and the Internet User (the End User accessing the Internet site) will receive an automatic alert web page. Notification of the denial of access to the web page or attachment also may be sent by email to the Administrator, if configured as part of the Web Protection Suite Service set-up.

1.4.2 **Web Filtering.** Once the relevant configuration changes are made and the Customer web traffic is routed to the Web Protection Suite Services, web pages and attachments will be filtered using URL categorization and content analysis. This process is called Web Filtering ("**WF**"). URLs are categorized by reference to a number of predefined categories as specified in the Portal.

The Administrator will configure WF to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet Users or groups. A number of additional features (e.g. 'blocked' and 'allowed' list functionality) are also available.

It may not be possible to filter certain web pages or attachments. The Administrator may configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through unless otherwise specified by the Administrator in relation to specific categories of content. WF will only filter web pages that are categorized by WF in accordance with the category that the Administrator has chosen to filter using the Portal.

The Administrator has the option of performing individual and/or group administration and reporting capabilities by utilizing the Connector Software, if this option is purchased. This will be agreed between the Orange and Customer as part of the setup for the Services.

If an Internet User requests a web page or attachment where an access restriction policy applies, then access to that web page or attachment will be denied and the Internet User will receive an automatic alert web page. Notification of the denial of access to the web page or attachment also may be sent by email to the Administrator, if configured as part of the Web Protection Suite Service set-up.

1.4.3 **Optional Services.** Customer may elect to receive the following optional services, subject to additional Charges.

1.4.3.1 **Instant Message Control.** The Instant Message Control ("**IMC**") service directs the End User's external Instant Message requests as prescribed by Orange (currently those used by Windows Live/.NET Messenger Service and Yahoo! Messenger), including all macros or messages, through the WPS Service. If ordered by Customer, the Administrator is responsible for making and maintaining the configuration settings required to direct this external traffic via the WPS Service based on Customer's technical IT Infrastructure. Once the relevant configuration changes are made, Instant Messages will be scanned by Instant Message spam analysis systems.

The Administrator will configure IMC to create access restriction policies based both on categories and types of content and deploy these at specific times to specific Internet Users or groups. Additional features (e.g. 'blocked' and 'allowed' list functionality, Instant Message protocol allowing/disabling) are also available.

It may not be possible to filter certain Instant Messages and any such messages will be blocked. Encrypted traffic cannot be filtered and will be passed through IMC unfiltered. IMC will only filter Instant Message content in accordance with the dictionaries that the Administrator has chosen to filter.

If an Internet User sends or receives Instant Message content for which an access restriction policy applies, then access to that Instant Message will be denied, and the Internet User will be displayed an automatic alert event. Notification of the access restriction to the content may also be sent by email to an Administrator, if configured as part of the Web Protection Suite Service set-up.

IMC will monitor and log Instant Message messages as well as making this information available through the Portal for the standard data retention period.

IMC will display notification messages concerning monitoring of Instant Messages as stipulated by the Administrator, if configured as part of the Web Protection Suite Service set-up.

1.4.3.2 **Connector Software.** If ordered by Customer, Orange will provide the Connector Software to Customer for deployment in Customer's IT Infrastructure, subject to installation guidelines. As an option, Orange can provide Customer the server hardware, software, and licensing in addition to the Web Protection Suite Service for installation of the Connector Software, subject to separate pricing.

The Connector Software enables End Users to connect to the Web Protection Suite Services even without a static IP address by using an authentication key. If End Users have other services that rely on a fixed IP address for identification, they can configure direct connections for specific websites, domains, hosts, or networks.

Administrators can create, revoke, activate, and deactivate authentication keys for Connector Software per group or per End User.

The Connector Software does not support all potential Customer or End User systems and set-ups.

1.4.3.3 **Secure Web Anywhere.** If ordered by Customer, Orange will provide the Secure Web Anywhere Software to Customer for installation on a PC or laptop in accordance with Orange installation guidelines.

Secure Web Anywhere allows the End User's PC or laptop to connect to the Services from a remote location outside the End User's internal network. Secure Web Anywhere does not rely on provisioned IP addresses.

Secure Web Anywhere does not support all potential End User setups. Orange will work with Customer during the sales engagement to determine the optimal and most appropriate integration design for each End User's IT Infrastructure.

1.4.3.4 **Block Alert Pages.** Block Alert Pages are dynamically generated HTML pages displayed to End Users when they are prevented from accessing prohibited web content. If ordered by Customer, the Administrator can choose a standard block alert page or Customer specific content which can be uploaded via the Portal and Orange will provide a user guide describing the operation of the Block Alert Pages.

1.5 Self Service Web Portal and Support

1.5.1 **Self Service Web Portal.** Customer's Administrator(s) and Super Users will be granted access to the Portal to administer and report on the Web Protection Suite Services. Access to the Portal is via a secure (https) website and is password-protected. This will only be provided to defined Administrators and/or Super Users as agreed by Customer and End User and communicated to Orange. If Customer has multiple Administrators for a single account, then Customer can give each Administrator a unique login and determine access privileges for each End User (e.g. full or read-only). This functionality allows a unique, single Super User account that can create multiple Administrators.

1.5.1.1 **Portal Functionality** enables the Administrator to:

- review statistics of all malware stopped and other web content blocked;
- create access restrictions and apply these to specific End Users or groups (if the Connector Software has been installed by the End User);
- customize browser alert pages seen by End Users when web access to a particular site or file is denied;
- update administration details for real-time email alerts; and
- configure and exhibit automated system auditing and reporting.

1.5.1.2 **Automated reports** are available on the Web Protection Suite Services, which may include overall traffic, bandwidth, blocked URLs, and web malware stopped. The Portal also offers a selection of additional reports that provide a more in-depth analysis using graphs, tables, or exportable data files. Administrator(s) can schedule regular reports for different service functionalities and specify End Users, times, and email it to certain End Users or groups. The Portal may not be able to provide certain any specific reporting requirements and/or procedures for individual End Users, and Customer should inquire as to any specific reporting needs/requirements prior the initial set-up.

1.5.1.3 **Audit Logging functionality** records administration, configuration, filtering, and policy changes made for the Web Protection Suite Services and can be configured by full access Administrator(s) or the Super User.

1.5.1.4 **Privacy Logging functionality**, when enabled, will log when web pages are blocked according to the applicable web filtering policy, but will obfuscate private details such as source username and IP address.

1.5.2 **Support**

1.5.2.1 **Support Activities.** Administrative support for the Web Protection Suite Service shall be provided via access to the Portal. However, Customer will contact the GCSC for any outage or non-availability of the Web Protection Suite Services or for support or guidance which cannot be offered by using the Portal.

Such support activities may include activities such as:

- assisting End Users in activating the Services;
- taking and logging all support calls and requests for help and/or assistance from End Users (both by telephone and by email) and providing assistance as appropriate;
- determining whether the call requires escalation to 2nd line support, and if so, referring the call to 2nd line support expert(s); and
- acting as interface with the End User for these reactive calls.

It is Customer's obligation to document and promptly report all errors or malfunctions of the Services to Orange. Customer is responsible for providing support information necessary for Orange to understand and resolve the incident. This information may include log files, configuration files, and error messages. Typical information required should be defined and provided to End Users by Customer so that this can be proactively communicated to the End Users prior to calls for support by End Users.

Orange does not guarantee that every question or problem raised by Customer will be resolved. The Orange success in resolving Incidents is conditional upon the willingness of Customer to follow the instructions with regards to installation, operation, and the use of the Services. Customer shall implement corrective actions and workaround procedures recommended by Orange to resolve the Incident and shall take all steps necessary to carry out any procedures Orange may give for the rectification of errors or malfunctions within a reasonable time after such procedures have been provided. Orange shall not be liable for any defaults in the Services which result from the failure of Customer to execute a supplied corrective action.

Orange reserves the right to close the ticket without further responsibility or liability if Customer does not provide appropriate feedback within 30 days of receiving new Services, a workaround for a problem, or fails to respond to a request for additional information.

The Orange obligation to provide support does not include services requested as a result of causes or errors that are not attributable to Orange or cannot be reproduced by Orange. Causes or errors that are not attributable to Orange include, but are not limited to, the following:

- negligent use, hardware malfunction, force majeure, or causes other than through ordinary or authorized use;
- modification or addition, or attempted modification or addition to the Services undertaken by Customer, End User or any person under their direct or indirect control;
- any software not licensed and/or provided by Orange.

1.6 Data Processing

Exhibit A sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and the categories of Data Subjects of the Processing of Personal Data carried out by Orange as part of this Service.

EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE BUSINESS SERVICES AS PROCESSOR FOR CUSTOMER - ARTICLE 28 OF GDPR

Name of the Service: Web Protection Suite

ExA.1 Processing Activities

Collection (receiving personal data of employees and users of customer who are natural persons, etc.).	Yes
Recording (capturing personal data in a file or software program, including the generation of metadata like Call Details Records, etc.).	Yes
Organization (organizing personal data in a software program, etc.).	Yes
Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.).	Yes
Modification (modifying the content or the way the personal data are structured, etc.).	No
Consultation (looking at personal data that we have stored in our files or software programs, etc.).	Yes
Disclosure or otherwise making available (communicating personal data to another recipient by any means, etc.). Except for disclosure mentioned in the service description or required by law, or otherwise specifically directed by the customer, the categories of potential recipients are only those subcontractors referenced herein or otherwise approved by the customer.	Yes
Combination (merging two or more databases with personal data, etc.).	No
Restriction (implementing security measures in order to restrict the access to the personal data, etc.).	Yes
Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.).	Yes
Other use (if "YES" to be detailed).	No

ExA.2 Categories of Personal Data Processed (Type of Personal Data)

Categories of Personal Data Identifiable by Orange	
Identification data (ID document / number, phone number, email, etc.).	Yes
Traffic / Connection data (IP address, Mac address, CDRs, access and usage data, online tracking and monitoring of services).	Yes
Location Data (geographic location, device location).	No
Customer Relationship Management data (billing information, customer service data, ticketing info, telephone recordings, etc.).	No
Financial data (bank account details, payment information).	No
Sensitive Data (racial/ethnic background, religion, political or philosophical beliefs, trade union membership, biometric data, genetic data, health data, sexual life, and/or orientation).	No
Categories of Personal Data Not Identifiable by Orange	
Any categories of personal data that may be recorded or stored (voicemail, call recording, files) by Customer and which recording is hosted on Orange infrastructure.	Yes

ExA.3 Subject-Matter and Duration of the Processing

Subject-Matter of Processing		**Duration of Processing**
Service activation.	Yes	For the period necessary to provide the service to the customer plus 6 months.
User authentication.	Yes	
Incident Management.	Yes	
Quality of Service.	Yes	
Invoice, contract, order (if they show the name and details of the contact person of Customer).	Yes	For the period required by applicable law.
Itemized billing (including traffic / connection data of end-users who are natural persons).	No	
Customer reporting.	Yes	For the duration requested by Customer.
Hosting.	Yes	For the duration of the hosting service ordered by Customer.
Other. [if yes please describe]	No	

ExA.4 Purposes of Processing

Provision of the service to Customer.

ExA.5 Categories of Data Subject

Customer's employees/self-employed contractors using or managing the service or the contract who are natural persons.	Yes
Customer's other end-users of the service who are natural persons (client of the Customer, etc.); usable by users other than internal users.	Yes

ExA.6 Sub-Processors

Sub-Processors Approved by Customer	Safety Measures
Orange Business Services entities that are processing information for this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services entities that are processing information for This Service and that are outside of the EU/EEA are communicated separately to the customer.	Intra-group agreements with standard model clauses, Binding Corporate Rules approval request filed with CNIL.
Orange Business Services suppliers which are performing one or more processing activities described above in connection with this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services suppliers that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the Customer.	Standard Model Clauses in contract with supplier.

END OF SERVICE DESCRIPTION FOR WEB PROTECTION SUITE