1 SERVICE DESCRIPTION FOR ACTIVE PREVENTION SERVICE

1.1 Definitions

As used in this Service Description, the following capitalized terms will have the meanings given to such terms in this Clause 1.1. 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.

"**Connection Kit**" means the CPE and associated Software provided by Orange and installed on a dedicated Ethernet port on the Firewall to establish the connections between the Customer Network and the SOC.

"**Customer Network**" means the Customer's telecommunications equipment (e.g. routers, switches, servers, etc.) monitored by the Active Prevention Service.

"**Customer Web Portal**" means the secure web site provided by Orange as part of and for Customer's Active Prevention Service.

"**Event**" means the detection of potentially unauthorized or malicious activity by a Sensor when incoming packet data traffic is matched to the Intrusion Detection Service signature database.

"**Incident**" means a fault, failure, or malfunction in the System.

"**Firewall**" means a method to enhance network security.

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

"**Maintenance Window**" means the recurring time interval mutually agreed upon by the Parties during which maintenance services on the Customer Network may be performed by Customer and during which temporary disruption or unavailability of the Customer Network or Sensors may occur.

"**Proper Operational Condition**" means the correct operational status of the System, as defined by the manufacturer or supplier of the System or as otherwise mutually agreed upon by the Parties, which includes the ability of the System to run its specified operating system software, but not applications software.

"**Security Dashboard**" means the dashboard on the management interface provided by Orange for the Active Prevention Service on which Orange will make available to Customer certain information and reports as described in this Service Description.

"**Security Policy**" means the policy that will be used by the SOC to classify Events.

"**Sensor**" means the CPE provided as part of the Active Prevention Service that is used to monitor the Customer Network for unauthorized or malicious data traffic. If Customer orders Intrusion Prevention, the Sensor also may be configured to block the unauthorized or malicious data traffic detected.

"**Sensor Policy**" means the security policy that is used by a Sensor to monitor data traffic on the Customer Network. If Customer orders Intrusion Prevention, then the security policy also may be used by the Sensor to block the unauthorized or malicious data traffic detected on the Customer Network.

"**Service Request Form**" or "**SRF**" means the form that details Customer's specific Active Prevention Service requirements as well as the Customer information needed and used by Orange to provide the Active Prevention Service, including a list of all equipment included in the Customer Network, the Customer Configuration Sheet, and Authorized Users Sheet, as described in Clause 1.2 below.

"**Severity Level**" means the category assigned by the GCSC for Incidents.

"**SOC**" means the security operating center from which the Security Monitoring Services (as described in Clause 1.5.1(b) below) are provided.

"**Software Patch**" means an officially released change to a Software program, generally an enhancement or logical complement to the current version of the Software program, that does not contain substantial new features or functions.

"**Software Upgrade**" means an officially released version of a Software program, which generally contains substantial changes, new features or functions.

"**System**" means the Software, CPE and other hardware provided by Orange as part of the Active Prevention Service, including the Sensors.

1.2 Service Obligations

1.2.1 Customer Requirements

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

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

1.2.2 Customer Security Contacts

Customer will identify a primary security contact and between 2 and 4 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 detected by Orange will be reported to the listed contacts, and Orange will respond only to Active Prevention Service requests and reports of Incidents issued by the listed contacts.

For Severity Level 1 and Severity Level 2 Incidents (as described in Clause 1.13), Orange will notify Customer's security contacts of the Incident using all contact details provided in the SRFs. For Severity Level 3 Incidents (as described in Clause 1.13), Orange will send a message to the email addresses set forth in the SRFs. All contacts will be made in English, unless otherwise agreed to between the Parties.

The primary security contact identified in each 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.

1.2.3 Customer Service Context

The SRF will include the Customer Service Context, and the Parties will revise the Customer Service Context as necessary during the Service Term to accurately reflect the status of the Active Prevention Service. The Customer Service Context includes the following:

(a) **Customer Configuration Sheets.** The Customer Configuration Sheet will identify the Maintenance Windows and Customer contact information for escalations, change management, Events, the Locations, support, and reporting.

(b) **Authorized Users Sheet.** Customer must specify all Users allowed access to the Customer Web Portal in the Authorized Users Sheet; Orange will provide the tokens needed to access the Customer Web Portal only for such Users. Orange will provide 2 tokens as part of the Active Prevention Service, and any additional tokens needed will be subject to additional Charges.

Customer must inform Orange of any change in its network that may impact the Active Prevention Service, including the addition or removal of servers or applications. Substantial changes to Customer's managed infrastructure should be implemented only during Maintenance Windows. Customer must inform Orange of such planned changes no less than 24 Business Hours before the change becomes effective. Customer must notify Orange of any unplanned change as soon as reasonably possible.

Customer acknowledges and agrees that if the procedure set forth in the preceding paragraph is not followed, interruptions of services or activities might occur or Orange may suspend the Active Prevention Service until the Customer Service Context is updated. Orange will not be liable for the payment of any Service Level credits or for any other liability under the Agreement to the extent that such credit or liability arises due to inaccuracies in the content of the Customer Service Context.

1.3 Scope of Services

Subject to Clause 1.4 below, Orange will provide the Active Prevention Service for Customer at the Location(s) and with the level of service (i.e. Standard, Enhanced or Extended) identified in each SRF. The Active Prevention Service includes Intrusion Detection, and Customer may order Intrusion Prevention as an option. Orange will provide, configure, install, perform acceptance testing on, and maintain the System provided as part of the Active Prevention Service.

Intrusion Detection monitors data packets directly from the Customer Network for Events, and Orange may analyze any Events detected and provide recommendations to Customer regarding such Events depending on the level of service ordered by Customer. If ordered by Customer, Intrusion Prevention will then block the unauthorized or malicious activity detected.

Except as otherwise expressly provided in this Service Description, to receive the Active Prevention Service at a Location, Customer also must provide an Internet connection and receive the Orange Secure Gateway Service (including an Orange-managed Firewall) at the Location. The Orange Secure Gateway Service will be described in a separate Service Description attached to this Agreement, and the Charges for such Service will be in addition to those for the Active Prevention Service.

1.4 Consulting and Service Deployment

1.4.1 Consulting Services

Prior to providing the Active Prevention Service, Orange will perform Consulting Services to analyze Customer's infrastructure, the equipment, and software for which Orange may provide the Active

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

Prevention Service, as well as Customer's security policies, to qualify and design the Active Prevention Service solution. The Consulting Services will be described in a separate Service Description attached to this Agreement or in a separate Letter of Engagement or Statement of Work executed by the Parties, and Charges for the Consulting Services are in addition to the Charges for the Active Prevention Service. Notwithstanding anything to the contrary contained in this Agreement, Orange will have no obligation to provide the Active Prevention Service if, as a result of the Consulting Services, Orange determines that it cannot provide the Active Prevention Service or the Parties do not agree on the implementation and design of the Active Prevention Service for Customer.

1.4.2 **Site Survey**

Promptly upon completion of the SRFs and prior to the deployment of the Active Prevention Service, Customer will perform a survey of the physical premises where the System will be installed (a "**Site Survey**"). Customer must gather the information requested in the Site Survey form provided by Orange for Orange to determine if the Location meets the necessary requirements for the proper installation and functioning of the System and to identify the specific tasks, if any, that Customer must complete to provide the Location with the proper infrastructure to support the System. Upon Customer's request and for an additional Charge, Orange will perform the Site Survey. If Orange performs the Site Survey, then a Customer representative must provide Orange with access to the Location and accompany the Orange personnel at all times during the Site Survey.

1.4.3 **Physical Environment Requirements**

Upon completion of the Site Survey, Orange will advise Customer of all Location preparation requirements that Customer must complete prior to the scheduled date for commencing installation of the System. If Customer fails to complete all such required preparations, Orange is relieved of its Active Prevention Service responsibilities at that Location until such time as it has been adequately prepared.

The Location must provide appropriate space, conditioned power, and environmental controls. The hardware components of the System have been designed to operate as a single unit and must be located within 3 feet of each other, or as otherwise directed by Orange.

Customer will be responsible for any damage to the CPE caused by incorrect power provisioning or electrical circuit overload. Additionally, Orange will not be responsible for any personal injury or property damage, including damage to Customer's equipment or network, that is due to incorrect power provisioning or electrical circuit overload. Customer also must provide:

- A secure location in which to install the System, accessible on a 24x7 basis.
- Appropriate space within a standard 19" rack, which rack also will include or be as close as reasonably possible to any equipment provided for other Orange Services to which the Active Prevention Service applies or is connected.
- 2 power outlets for the Connection Kit and 1 power outlet per installed Sensor, which are 110V/60Hz conditioned power outlets (or 220V / 50Hz as appropriate for the applicable country) and installed within 3 feet of the System.
- An Ethernet connection to Customer’s internal IP-based Local Area Network for each Sensor.
- An available Ethernet port on the Firewall.

1.4.4 **Lead Time Requirements**

The System will be deployed within 10 weeks from the date on which the SRF is received and signed by Orange, and such deployment will be delayed if Customer requires changes to the specifications listed in the completed and accepted SRFs.

1.4.5 **Configuration**

Orange will configure each System wholly 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 plus Expenses for such services.

Upon completion of the configuration, the System will be delivered to the Location specified in the SRF. Customer will visibly inspect the exterior condition of the System packaging prior to accepting delivery. After accepting delivery, Customer will store the System in a secure location until Orange commences installation. Customer will bear the risk of loss while the System remains at the Location.

Following installation and acceptance testing, Orange will accept requests for changes to the configuration of the System only from the security contacts identified in the SRF. All such changes will be subject to verification by Orange in accordance with mutually established procedures agreed to in writing by the Parties prior to the commencement of the Active Prevention Service.

1.4.6 **Installation**

Before Orange will install the System, Customer must provide written confirmation that the following tasks have been completed:

(a) Satisfactory delivery of the System to the Location;

(b) All data circuits are installed and operational; and

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

(c) The Location has been properly prepared in accordance with Clause 1.4.3 and the Orange direction pursuant to the Site Survey.

Orange will install the System upon its receipt of Customer's confirmation. Unless otherwise agreed to by the Parties, System installation will be conducted during Business Hours. If Customer requests Orange to install the System outside of Business Hours, then Orange will advise Customer of any increased charges prior to commencement of the installation.

Orange will not be responsible for any delay in the installation of the System if such delay is due to any cause beyond its reasonable control, including the inability by Orange to gain access as scheduled to the Location, failure by the local access provider to complete installation of the circuits, or Customer's failure to properly prepare the Location.

Orange will contact Customer at least one day prior to the scheduled installation date to confirm the installation appointment. If Orange determines that the Location has not been appropriately prepared and that Orange cannot install the System, then Orange will notify Customer promptly, and Orange will have no responsibility to continue with the installation. However, if the designated Customer contact disagrees with the Orange assessment that the Location has not been properly prepared, the Parties will escalate the issue promptly in accordance with the escalation procedures set forth in the General Conditions. Customer will advise Orange when the Location has been properly prepared, and the installation will be rescheduled based upon the preparation activities required. If, as a result of rescheduling, Orange must make more than one trip to the Location or remain at the Location and wait for the Location to be adequately prepared, then the additional time required will be billed at the Hourly Labor Rate, plus Expenses.

As part of the installation, Orange will interconnect the System to the demarcation and to the Customer Network and will notify Customer promptly if any problems occur during installation that adversely affect the installation process. At least one Sensor must be installed behind the Firewall at each Location; Sensors installed outside of the Firewall will be used only for reporting and correlation (i.e. no Event alerting or recommendations will be provided for such Sensors).

1.4.7 **Installation Phases**

Orange will install the Active Prevention Service in the following 2 phases:

(a) A Connectivity Testing Phase to validate connectivity of the Sensor to the customer Network and to the SOC. Upon completion of this phase, Orange will deliver a Service Ready for Fine-Tuning notification, and Customer will be invoiced for all one-time Charges associated with the Active Prevention Service; and

(b) A Fine-Tuning and Information-Gathering Phase, which may last 2 to 3 weeks, to establish and confirm the accuracy of the Customer Service Context, Sensor Policy and the Sensor Software. Upon successful completion of this phase, Orange will deliver to Customer a Ready for Service Notification, at which time any applicable Service Levels or Service Level Objectives may apply and Customer will be invoiced for the first monthly recurring Charges.

1.4.8 **Acceptance Testing**

Upon completion of the installation of the Active Prevention Service, Orange will commence acceptance testing to confirm that all aspects of the System and the Active Prevention Service are operational in accordance with the terms set forth in this Service Description and the parameters set forth in the SRFs (e.g. verifying the IP addresses, ensuring that the Sensor Policy configurations have been successfully loaded and that the activated features on the System are performing as defined in the SRFs).

Upon completion of the acceptance testing, Orange will provide to Customer an "**Active Prevention Service Acceptance**" form for each System installed for Customer's execution. Customer will be deemed to have accepted the Active Prevention Service on the date on which Orange issues the Active Prevention Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Active Prevention Service within 5 Business Days of receipt of the Active Prevention Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.5 Description of Services

Customer will receive the Standard, Enhanced, or Extended Intrusion Detection Service, as specified in the Order.

1.5.1 **Standard Intrusion Detection**

(a) **Proactive System Monitoring.** Orange will proactively test each Sensor by executing a ping command at various intervals. If a Sensor does not respond within a defined amount of time, a non-availability alarm will be generated. Orange will notify Customer of such alarm in accordance with the Customer Service Context when the alarm has been received by Orange.

(b) **Security Monitoring.** Orange will monitor the Customer Network via the Sensor 24 hours a day, 7 days a week for Events as and when these become available at the SOC. Orange will evaluate and classify the Events based on the location of the Sensor and identification of the attack.

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

1.5.2 **Enhanced Intrusion Detection**

With Enhanced Intrusion Detection, Customer will receive the Standard Intrusion Detection Service as well as a detailed analysis by the SOC of Events that are considered "critical" or "Level 1" based on the Security Policy and associated recommendations for modifying or updating the Sensor Policy. The analyses and recommendations will be provided to Customer via email every 2 weeks.

1.5.3 **Extended Intrusion Detection**

With Extended Intrusion Detection, Customer will receive the Enhanced Intrusion Detection Service, except that the SOC will alert Customer of Events on a near real-time basis and provide the analyses and associated recommendations for modifying or updating the Sensor Policy 24 hours a day, 7 days a week.

1.6 Fine-Tuning Phase

During the Fine-Tuning phase, there is a risk that genuine, authorized traffic will falsely trigger the Sensors, causing an excessive number of Events. Therefore, during this phase, the SOC will investigate Events in an effort to eliminate false positives, and no blocking action will be configured.

Customer hereby authorizes Orange to make changes to the Security Policy and the Sensor Policy during the Fine-Tuning Phase without prior consent of Customer, provided that Orange notifies Customer in writing within 4 Business Hours of any change it makes and that Orange does not re-classify any Events without Customer's prior written consent.

1.7 System Management

1.7.1 **Software Upgrades**

Orange will provide version management of the operating system and various elements of the Active Prevention Software. Software Upgrades may include the addition of Software Patches to the operating system that are of a security nature and those that would affect the operation of the Software. The upgrade to a new operating system level also will be made if Orange deems it necessary for security reasons or for support of the Software. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the hardware vendors and Software licensors, and Orange, in its sole discretion will decide when upgrades take place.

Customer will be informed of Software Upgrades through the Customer Web Portal. Software Upgrades will be done during Maintenance Windows and will be installed remotely. If Orange needs to take a System off-line to implement Software Upgrades or network enhancements, Orange will provide Customer with at least 7 days prior written notice thereof. When possible, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement System upgrades remotely during Business Hours. If Orange is required to install an upgrade at the Location, or outside of Business Hours, Customer will be charged at the Hourly Labor Rates for such services, plus Expenses.

1.7.2 **Sensor Back-Up**

Orange will store the current configuration of the Sensors. In case of a failure in a Sensor, Orange will:

(a) restore the latest available Sensor Policy on the Sensor;

(b) restore the secure connection to the SOC;

(c) install the latest version of the operating Software (including previously installed Software Patches); and

(d) install the Sensor Software. Orange will maintain, and may construct, a back-up from incremental back-ups of the Sensor Policy, configuration data, and copies of the original Software and any Software Upgrades and Software Patches installed on the Sensors.

Orange will have no responsibility for the back-up of or for the Customer Network, including any software.

1.8 Security Management

1.8.1 **Software Patches and Security Threats**

Orange checks for new security threats and corresponding Software Patches, including new Sensor signatures, daily. If a new security Software Patch is available, Orange will inform Customer no later than 24 Business Hours after discovery through the Customer Web Portal. Software Patches are installed remotely; however, if remote installations are not possible, Orange will perform these installations on-site at the Hourly Labor Rates plus Expenses.

If Orange determines that the associated security threat is critical, the Software Patch installation will be scheduled for one of the next available Maintenance Windows. If Orange determines that the associated security threat is non-critical, the Software Patch will be scheduled with the Software Upgrades described in Clause 1.7.1.

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

1.8.2 **Policy Change Requests**

Orange must approve and will manage the Security Policy and Sensor Policy, but Customer will maintain ownership of and responsibility for the content of such Policies and will approve the initial Security Policy and Sensor Policy, and all changes thereto, except as set out in Clause 1.6 (Fine-Tuning Phase). However, Customer authorizes Orange to modify the Security Policy and the Sensor Policy without Customer's prior consent if the SOC receives an excessive number of Events; provided that Orange notifies Customer in writing within 4 Business Hours of the change to the Sensor Policy or the Security Policy and that Orange will not reclassify any Events (in accordance with the Security Policy) without Customer's prior written consent.

All Customer change requests to the Sensor Policy or Security Policy must be entered via the Customer Web Portal using the structured or unstructured forms, as applicable, made available on the Customer Web Portal. Customer may request a maximum number of 5 change folders per month; except as otherwise identified by Orange, a change folder is composed of a maximum of:

(a) 30 Sensor Policy rule changes, including additions, removals, or modifications. Examples include:
  (i) Changing the action for a Sensor Policy rule (e.g. "**log-only**" to "**drop connection**");
  (ii) Adding or removing servers to the Customer Network;
  (iii) Adding or removing a maximum of 30 network objects in the Customer Network; and
  (iv) Adding or removing attacks or attack groups detection.

(b) 30 changes to the Customer Network to which the Sensor Policy applies, which may include:
  (i) Adding or removing servers to the Customer Network;
  (ii) Adding or removing a maximum of 30 network objects in the Customer Network;
  (iii) Adding, removing, or upgrading the operating system of the Customer Network;
  (iv) Adding, removing, upgrading, or providing a patch for Customer applications.

Orange will provide Customer with analysis and feedback relating to the requested change within 24 Business Hours through the Customer Web Portal, and any change to the Customer Network may require a Sensor Policy change. If Orange determines that there is insufficient data available to conduct and complete the analysis, Orange will request Customer to provide additional information. Customer must be available by telephone to clarify and explain the details of the change request and follow up with written confirmation of the decisions made during the phone call.

If, in the opinion of Orange, Customer's change request could introduce security risks, Orange will require Customer's prompt written acknowledgment and acceptance of such risks by Customer before implementation. By providing acknowledgement and acceptance of such risks, Customer agrees that interruptions of services or activities may occur due to the implemented changes. Orange will post the agreed date and time of the change request implementation on the Customer Web Portal.

1.9 Optional Features

Subject to additional Charges, Customer may order the following optional features for the Active Prevention Service.

1.9.1 **Intrusion Prevention**

If Customer orders Intrusion Prevention as part of the Active Prevention Service, then the System will be configured so that all data on the Customer Network subject to the Active Prevention Service will flow through the Sensor, which will screen and attempt to block any data traffic triggering an Event in compliance with the Sensor Policy.

1.9.2 **High Availability**

Orange will provide 2 Sensors that will work together as a cluster in either active/active mode (i.e. both Sensors working simultaneously at all times, implying load balancing between the 2 Sensors) or active/passive mode (one Sensor acts as the master and the other as a backup, with the 2 Sensors continuously sharing state and configuration data).

1.9.3 **Stand-alone**

Subject to the Orange approval, Customer may order the Active Prevention Service without receiving the Orange Secure Gateway Service. In such event, Orange will identify in writing the requirements that Customer must meet (including any services (e.g. firewalls) or equipment that Customer must provide) to enable Orange to provide the Active Prevention Service, and Orange will provide a dedicated management solution to remotely manage the Sensor(s). Orange will not be responsible or liable for:

(a) any services or equipment that Customer provides for use with the Active Prevention Service,

(b) any fault in or failure of the Active Prevention Service caused by such Customer services or equipment, or

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

(c) any fault in or failure of Customer services or equipment caused by the Active Prevention Service.

1.10 Reporting

Customer may access near real-time reports regarding Events directly on the Security Dashboard using a secured SSL VPN connection; the Event information will be available on the Security Dashboard for up to 24 hours. Customer also may access reports via the Customer Web Portal, which may include, among others:

- Top 100 attacks;
- Top 20 attackers;
- Top 20 targets; and
- Attacks by severity.

The reports available on the Customer Web Portal will be posted on a weekly and monthly basis.

1.11 Customer Obligations

1.11.1 Connection

For Orange to provide the Active Prevention Service, Customer must be connected to the SOC using an infrastructure that guarantees "**Quality of Service**" (i.e. via encrypted Internet access over a leased-line). As part of the Consulting Services and upon configuration of the Sensor, Orange will advise Customer of the bandwidth required, and Customer will provide such bandwidth for use with the Active Prevention Service. If the infrastructure provided by Customer does not guarantee the required "**Quality of Service**", Orange will notify Customer of such, and Orange will not be liable or responsible for any failure in the Active Prevention Service as a result thereof.

1.11.2 Customer Network

Customer will coordinate with Orange the upgrade, replacement, or back-up of any equipment on the Customer Network that may be performed by or on behalf of Customer. If Customer restores or backs-up such equipment, then Customer also will restore the connection between the Customer Network and any other connection not restored by Orange pursuant to Clause 1.7.2 above. In addition, Customer will provide an external authentication service if the number of Users exceeds 5.

1.12 Pricing

Charges for the Active Prevention Service may be based on the nature of the Location and include a monthly recurring Charge and one-time set-up Charges for account set-up, connectivity set-up, and Sensor set-up. Additional Charges also will apply to the optional features ordered by Customer.

1.13 Maintenance of the System

1.13.1 Remedial Maintenance

Orange will maintain the hardware portion of the System in Proper Operational Condition. If an Incident is caused by a failure in the System hardware, Orange will repair the Incident following receipt of a report of the Incident from Customer or detection of the Incident by Orange, whichever first occurs. If Orange is unable to restore the System hardware to Proper Operational Condition remotely, an Orange field engineer will be dispatched to the Location. If an Incident was not caused by Orange, then the resolution of the Incident will consume one Service Ticket.

The GCSC will classify all Incidents as follows:

(a) **Severity Level 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.

(b) **Severity Level 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.

(c) **Severity Level 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

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL

1.13.2 **Remedial Maintenance Exclusions**

Orange will have no obligation to furnish Remedial Maintenance Services for, nor will Orange be liable to Customer for damages of loss of the Active Prevention Service or the System caused by any of the following (collectively "**Limitations**"):

(a) Damage to the System caused by temperature or electrical current fluctuation, or any Force Majeure Event, or any other casualty or loss;

(b) Damage caused by adjustments and repairs made by persons other than Orange own representatives, its Subcontractors, or personnel approved in writing by Orange; or

(c) Any instabilities in the operation of the System that are caused by or related to the use of certain software, or by any other software provided by Customer or its designees, or by combinations of the System and software, even if such combination is specified on a duly accepted SRF, or by any hardware connected to the System.

Reports of Incidents from Customer 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.

Remedial Maintenance Services do not include:

- Electrical work external to the System, except as otherwise set forth in this Service Description;
- Maintenance of attachments or other devices not specified in the SRFs;
- 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; or
- Failure by Customer to meet the physical and environmental specifications for System.

Any visits to a Location or repairs to the System made necessary by the preceding causes will be charged to and paid by Customer at the Hourly Labor Rate plus Expenses.

END OF SERVICE DESCRIPTION FOR ACTIVE PREVENTION SERVICE

Orange and Orange Business Services are trading names of the Orange Group and are trademarks of Orange Brand Services Limited.
CONFIDENTIAL