TATA COMMUNICATIONS

MANAGED ADVANCE ENDPOINT SECURITY SOLUTION WEB MODULE

Part I. GENERAL TERMS

1. **Applicability**.

This document and all attachments incorporated by reference form the managed advance endpoint security Service Schedule ("**Service Schedule**"). To order the Services making up the Tata Communications managed advance endpoint security Solution ("**Solution**"), the Parties must execute an Order Form that expressly incorporates: i) this Service Schedule, and ii) a General Terms and Conditions or Master Services Agreement document ("**GT&Cs**" or "**General Terms**"). The GT&Cs, Service Schedule, and Order Form, and all other documents they incorporate by reference, constitute the "**Managed Advanced Endpoint Security Solution Agreement**" or "**Solution Agreement**". The Solution Agreement governs the delivery and Customer's receipt of the Solution.

2. **Managed Services Sub-Options**.

These Services are available in two sub-options: (i) mAES Standard; and (ii) mAES Premium. Features available under each of these options are provided below:

Managed Service Offering	Standard	Premium
Availability monitoring & management of vendor Software	✔	✔
Performance monitoring & management of vendor Software	✔	✔
Backup management of the configuration file (which may include policy configurations, definitions, versions etc.)	1 Month	3 Months
Number of policy or configuration (relating to settings) changes per month	5	10
Number of emergency policy changes per month	1	2
Maintenance window for policy/configuration changes	✔	✔
Vendor Software updates & Patch management	✔	✔
Customer portal access	✔	✔
Security event monitoring and notification (as specified in point 3 below)	✘	✔
Detailed security event reporting (as specified in point 3 below)	✘	✔
Reports		
Standard Reports (available on the customer portal)	✔	✔
Customized Reports (available on the customer portal)	✘	✔
Log archival (Customer shall provide the storage)	✘	✔
Policy change request implementation SLA	12 Hrs	8 Hrs
Customer service portal uptime	99.99%	99.99%

In the above table, ✘ means this offering is not available and ✔ means this offering is available.

3. **Security event monitoring and notification.** The security event monitoring involves threat incident identification (in accordance with Supplier's pre-defined parameters) and notification of such incidents to the SOC on a 24x7 basis. Additionally, all such security incidents will be reported to the Customer on a periodic basis as determined by Supplier or on a request basis as mutually agreed between Parties from time to time.

4. **Service Limitations**. The Services are not warranted to operate uninterrupted or error free. New security threats are constantly evolving, and no product or Service designed to provide protection from such threats will be able to insulate network resources from all security threats and vulnerabilities, and there are no guarantees against unsolicited e-mails and undesirable Internet content. Products and Services are not fault tolerant and are not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which product or Service failure could lead to death, personal injury, or property damage. Customer acknowledges products or Services for testing, assessing, scanning or monitoring the security of network resources, including implementation and deployment, may disclose or create problems in the operation of such resources; therefore, Customer and its employees and agents represent and warrant that (i) they are fully authorized by the Customer and the owners of the network resources to enter into this Agreement and each Order Form, and (ii) they and the owners of such network resources understand and accept the risks involved which in some circumstances could include without limitation, down time, loss of connectivity or data, system crashes or performance degradation.

5. **Use of Third Party Products**. Use of Third Party Product(s) (defined below) supplied hereunder, if any, will be subject solely to the third party's terms and conditions which will be provided to Customer upon delivery. Supplier will pass any Third-Party Product warranties through to Customer to the extent Supplier is authorized to do so. Customer agrees to indemnify, defend and hold Supplier, its officers, directors, employees, Affiliates and suppliers harmless from any claims, losses, damages, penalties or costs (including, without limitation, reasonable attorneys' and expert witness fees) arising out of any claims that Customer's use of the Services violates the rights of any third party in Third Party Product or the vendor Software. "Third Party Product(s)" means any software and/or hardware including the vendor Software which are supplied to Customer under this Solution Agreement, but which are not produced by Supplier. Third Party Products may include hardware, software and other related products.

Part II. DEFINITIONS

1. **Definitions**. Capitalized terms used in this Service Schedule but not otherwise defined herein shall have the meanings given to them in the GT&CS.

"**CPE**" means Supplier Provided Equipment or Customer Equipment, as the case may be.

"**Definition Update**" means any regular updates to the vendor Software on the Endpoints as are made available by the applicable vendor from time to time.

"**Emergency Change Request**" means any change request to be carried out to remediate a Severity 1 incident.

"**Endpoints**" means the endpoint infrastructure used or subscribed by Customer where the Services are being provided by the Supplier and where such Endpoint is connected to the Internet.

"**Endpoint Management Console**" means a centralized user interface application to secure and control the Endpoints.

th"**Internet Emergency**" means an incident which has affected a significant portion of protected Customer's Networks or the public internet and which affects connectivity to the Endpoint Management Console.

"**ITSM**" means Information Technology Service Management.

"**Monthly Recurring Charge**" or "**MRC**" means the monthly recurring charges for the Service as set out in the Order Form.

"**Network**" means any telecommunication network.

"**Non-Recurring Charge**" or "**NRC**" means the non-recurring charges for installing, commissioning and provisioning of the Service as set out in the Order Form.

"**Outage**" means any event or circumstance which results in non-conformance to the agreed upon SLA Targets.

"**Patch**" or "**Patches**" means the process of repairing vendor Software vulnerabilities which are discovered after the vendor Software has been deployed for the Customer.

"**Planned Maintenance**" means any preventative, routine or scheduled maintenance which is performed with regard to the Service, or any component thereof, which Supplier or its agents reasonably believe is necessary in order to maintain the Service or prevent or remedy a defect which may affect Customer's use or access to the Services. Supplier shall endeavor to give Customer at least a seven (7) day notice of any Planned Maintenance event.

"**Qualifying Incident**" means an Outage for which Customer raises a Trouble Ticket and which are confirmed by Supplier as a fault or Service degradation.

"**RGA Process**" means return of goods authorization process under which a product is returned to the supplier either to be eligible for a refund, replacement, or repair during the product's warranty period, in accordance with supplier's policies.

"**Security Contacts**" means Customer's representatives identified either under the COF or as may be communicated in writing to the Supplier from time to time.

"**Service Availability**" means the percentage of time that the Service is available.

"**Service Credits**" means credits provided by Supplier to Customer for not meeting the Service Availability or failure to meet other Service Level Targets as set out herein.

"**Service Credits Exceptions**" means any of the following circumstances either individually or together:

a) If Security Contact information is out of date or inaccurate due to Customer action or omission, Supplier will be relieved of its obligations under the SLAs and all remedies set forth herein are considered null and void.

b) If Customer fails to notify Supplier as stated in Clause 3(ii) of the Customer Responsibilities under the Service Schedule, Supplier will be relieved of its obligations under the SLAs and all remedies set forth herein are considered null and void.

c) If any SLA failure is attributable to non-Supplier managed Customer Premises Equipment hardware and/or software failure, including any and all security platform failures, Supplier will be relieved of its obligations under the SLAs and all remedies set forth herein shall be considered null and void.

d) Miscellaneous: If any SLA failure is attributable to below events, Supplier will be relieved of its obligations under the SLAs and all remedies set forth herein shall be considered null and void:

(i) Delay in CRFS Date caused (i) by Supplier having to obtain rights-of-way from any third party to access Site or Customer Premises, or (ii) due to Customer dependency like Site or Customer Premises not being ready for installation, delivery and supply of Services, roof right permissions / approvals not in place etc.;
(ii) Incorrect data or Site or Customer Premises information provided by Customer to Supplier;
(iii) Any act or omission of Customer or any of its agents, contractors or vendors, including failure of Customer to initiate Trouble Ticket or where Customer does not release the Service to Supplier for testing;
(iv) Force Majeure Events including without limitation, outages on the Internet;
(v) Planned Maintenance on the Customer infrastructure or Network;
(vi) delay or failure by Customer to perform recommended upgrades or download recommended software Patches or Definition Update;
(vii) delay or failure by Customer to provide accurate or complete data or information required by Supplier to provide the Services; or
(viii) any Service impact as a result of configuration provisioned by the Customer which is not attributable to Supplier.

"**Service Level Target**" or "**Service Availability Target**" or "**SLA**" or "**SLA Target**" means the offered minimum level of performance for the relevant parameter of the Services.

"**Severity 1**" means a critical problem that stops the Service from functioning. Examples include where the Service is significantly impaired and affects 10 or more Endpoints with the same malware within the same hour.

"**Severity 2**" means a problem with a severe impact on Customer's use of the Service, but does not stops it from functioning. The Service is interrupted or severely degraded and Customer is not able to work at expected levels of performance. Examples include where the Service is marginally impaired and affects limited set of Endpoints (5-9 Endpoints) of the Customer and may also impact the availability of the Endpoint Management Console or ability to distribute any Definition Updates.

"**Severity 3**" means a minor problem that does not seriously affect the Service. Examples include where the Service affects a limited set of Endpoints (less than 5 Endpoints) with the same malware within the same hour or where the Endpoints are not updated with any Definition Updates.

"**Site**" means a site owned or controlled by the Customer.

"**Trouble Ticket**" means the official method used by Customer to advise Supplier of a potential Outage.

[**End of Text**]