Service Specific Terms

Trend Micro Professional Services

Vodafone Business Customers

THE PARTIES AGREE:

1. Structure of contractual relationship

1.1 This Professional Services Agreement (this **"Agreement"**) incorporates the following terms and conditions:

1.1.1. The agreed statement of work (the **"SOW");**

1.1.2. The Professional Services General Terms, which can be found at www.vodafone.co.uk/terms, govern the relationship of the Parties in relation to any Service provided by Vodafone to the Customer under the SOW; and

1.1.3. The Vodafone Business Marketplace Service Specific Terms (the **"VBM Service Terms"**), which can be found at www.vodafone.co.uk/cloudservices/.

1.2 Precedence: In the event of any conflict between the provisions of (a) the SOW; (b) the VBM Service Terms; and (c) the Professional Services General Terms, this decreasing order of precedence shall apply.

2. Vodafone Business Marketplace (the "Marketplace")

2.1 The Service is made available to purchase through the Marketplace.

2.2 The VBM Service Terms apply to the extent of the Customer's use of the Marketplace website.

2.3 The Customer accepts that certain features and functionality detailed in the VBM Service Terms may be limited or not apply to the Service, including but not limited to the applicability of Charges and Subscription periods.

STATEMENT OF WORK

STATEMENT OF WORK ("**SOW**"): **Vodafone Managed Professional Services: Trend Micro (the "Service")**

1. Project and Services – Trend Micro Professional Services (the "Service")

<table>
<tr>
<td><b>Service Summary</b></td>
<td>The aim of the service is to configure and deploy the required service/s within the customers environment. This will include configuration of the customers Trend Micro portal/s, deployment and activation of the Trend Micro services, and best practices.

There are two Professional Services packages available, which are designed to support the onboarding of 3 Trend Micro Licences.

<table>
<tr><th>Trend Micro Licence</th><th>Professional Service Package</th></tr>
<tr><td>Worry Free Services</td><td>Trend Micro Standard Onboarding Package</td></tr>
<tr><td>Worry Free Services Advanced
OR
Worry Free XDR</td><td>Trend Micro Advanced Onboarding Package</td></tr>
</table>
</td>
</tr>
</table>

Customer Prerequisites and Responsibilities

Whilst the changes required to enable the service would be achieved in partnership with Vodafone, the Customer environment and the changes remain the responsibility of the Customer.

Depending on the service, some or all the following items may be relevant.

- Customer to provide full details of any existing service that provides similar services.
- Customer is responsible for all communications to end users.
- Customer is responsible for the removal of the product currently providing the Service.
- Customer is responsible for the modification of the MX records.
- Customer to provide access to Mobile Device Management (MDM) platform for integration purposes. The Customer takes responsibility for changes made to the MDM.
- Customer is responsible for changes required for integration with their Microsoft 365 tenancy.

Service Methodology

The Service will be provided by Vodafone Professional Services team based in the UK.

The Trend Micro service portal/s will be provided, hosted, maintained and supported by Trend Micro.

The Customer would select the service depending on their requirements. The Vodafone Professional Services team could work with the customer to configure the Trend Micro service portal/s to meet the customer requirements. The Trend Micro Endpoint application activation method would be agreed as part of the delivery.

Worry Free Services – Endpoint Security

- Endpoint Administration/Configuration/Deployment

Worry Free Services Advanced

- Endpoint Administration/Configuration/Deployment
- Cloud App Security
- Email Security

Worry Free XDA

- Endpoint Administration/Configuration/Deployment
- Cloud App Security
- Email Security
- Extended Detection and Response (XDR)

Customer Deliverables

The following deliverables are available to the Customer depending on the licenses purchased and the Customer requirements:

Professional Service Package	Deliverables
Trend Micro Standard Onboarding Package	**Deliverable 1:** Trend Micro configuration and deployment. **Deliverable 2:** Trend Micro Customer Integration. These deliverables cover: **Install Endpoint Agent** - Install the Security Agent to protect your endpoints from security threats. You can download the installer or send the installer link to users. **Configure Policies by OS** - Configure and apply security settings to specified targets. Use policies to manage settings such as Scheduled Scan, Device Control, and Data Loss Prevention. Threat Protection • Scan Settings • Behaviour Monitoring • Predictive Machine Learning • Vulnerability Protection • Web Reputation

			• Firewall • Endpoint Sensor • Sample Submission Data Protection • Device Control • Data Loss Prevention Access Control • URL Filtering • Application Control Exception Lists • Scan Exclusions • Approved/Blocked URLs Agent Configurations • Privileges and Other settings **AD Integration** - Integrate your Active Directory to manage Security Agents easily. You can also discover unmanaged endpoints that have no Security Agent installed. Azure AD/OnPrem AD supported.	
		Trend Micro Advanced Onboarding Package	**Deliverable 1:** Trend Micro configuration and deployment. **Deliverable 2:** Trend Micro Customer Integration. These deliverables cover in addition to what is included with Trend Micro Standard Onboarding Package: **Email Security** **Email Domains** - Management of internal Domains for mail flow and security: • Inbound and Outbound Protection • Managing Recipient Filter • Managing Sender Filter • Transport Layer Security (TLS) Peers • Understanding IP Reputation • Domain-based Authentication • File Password Analysis • Configuring Scan Exceptions • High Profile Domains • High Profile Users • Configuring Time-of-Click Protection Settings **DLP** - Data Loss Prevention (DLP) safeguards an organization's digital assets against accidental or deliberate leakage. DLP evaluates data against a set of rules defined in policies to determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission. With DLP, Trend Micro Email Security allows you to manage your incoming email messages containing sensitive data and protects your organization against data loss by monitoring your outbound email messages. **Connection filtering Inbound/Outbound** - Trend Micro Email Security provides inbound message protection by evaluating email messages in the following order: **Connection filtering** - Provides the recipient filter, sender filter, Transport Layer Security (TLS) check, and IP Reputation settings. Domain-based authentication - Provides authentication methods such as Sender IP Match, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect against email spoofing.	

Virus scan - Allows you to configure virus policies and scan exceptions.

Spam filtering - Allows you to configure spam policies, high profile users for BEC policies and Time-of-Click Protection settings.

Content filtering - Allows you to configure content filtering policies to take actions on messages based on the conditions matched.

Data Loss Prevention - Allows you to create Data Loss Prevention (DLP) policies to manage your incoming email messages containing sensitive data.

Quarantine - Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered on the administrator console. Furthermore, end users can view and manage their own quarantined messages on the End User Console.

Mail Tracking - This screen is designed for you to track email messages that passed through Trend Micro Email Security, including blocked or delivered messages. Trend Micro Email Security maintains up to 90 days of mail tracking logs. The sliding window for mail tracking log search is 60 continuous days that may cross calendar months

Cloud App Security

Services - Exchange Online, OneDrive, SharePoint Online, MS Teams, Teams Chat, Gmail, Google Drive, Box, Dropbox, Salesforce Sandbox, Salesforce Production
Svc Accts - Create a service account for each protected cloud service and grant Cloud App Security limited access to your service data for threat protection.

DLP - With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure. Data Loss Prevention safeguards an organization’s sensitive data against accidental or deliberate leakage.
Policies - Configure and apply policies to protect your users against various security threats and unauthorized transmission of sensitive data.

Administrator and Role - Specify users as administrator, manage custom administrative roles, and reset passwords for the administrators.

Global Settings
Approved Exchange Online Users - Approved Exchange Online users are used to specify the Exchange Online users whose email accounts will be excluded from scanning during policy enforcement when the user is selected as a target in the corresponding policies. A maximum of 1024 approved users are supported.

Approved Header Field List for Exchange Online - Approved Header Field List for Exchange Online specifies the header field criteria for email messages in Exchange Online to bypass policy scanning when a message match any of the criteria. A maximum of 10 header fields is supported.

Approved Header Field List for Gmail - Approved Header Field List for Gmail specifies the header field criteria for email messages in Gmail to bypass policy scanning when a message match any of the criteria. A maximum of 10 header fields is supported.

			Blocked Lists for Exchange Online - Blocked Lists for Exchange Online specify the blocked senders, URLs, SHA-1 hash values, and SHA-256 hash values through the Threat Remediation API. Email messages that match any item in the lists will be quarantined by Cloud App Security. A maximum of 2048 items in each list is supported. **Notification Email Settings** - Customize the signature for notification email messages **High Profile Domains** - High profile domains are used to specify legitimate sender domains that might be frequently forged into cousin domains for spam, phishing, and BEC attacks. A maximum of 100 high profile domains is supported. **Internal Domains** - Internal domains are used to distinguish incoming email traffic and can be added to the approved URL list to exclude from Web Reputation scanning. **High Profile Users** - High profile users are used to specify the email display names of the users who might be frequently forged for BEC attacks. A maximum of 1000 high profile users is supported. **High Profile User Exception List** - High Profile User Exception List specifies the email addresses to skip from scanning for writing style verification. For example, personal email addresses of high profile user(s), or system email addresses to send system-generated notifications. A maximum of 500 email addresses is supported. **Predictive Machine Learning Exception List** - Predictive Machine Learning Exception List specifies the SHA-1 hash values of files to exclude from scanning by Trend Micro Predictive Machine Learning. A maximum of 500 SHA-1 hash values is supported. **Suspicious Object List** - Trend Micro Vision One / Apex Central / Control Manager consolidates your organization's Suspicious Object lists and synchronizes the suspicious URL and file lists with the integrated managed Cloud App Security. Enable this feature to implement the lists during scanning **Display Name Spoofing Detection Exception List** - Display Name Spoofing Detection Exception List specifies the external senders to skip from display name check for email impersonation attacks. A maximum of 500 email addresses is supported. **Time-of-Click Protection Settings** - Time-of-Click Protection Settings specify actions on URLs at each risk level classified by Web Reputation Services every time a URL is clicked **Single Sign-On** - Configure SAML settings for single sign-on from your corporate portal or identity provider to Cloud App Security Where customer has Worry Free XDR: **Endpoint Sensor** – Enable the monitoring and investigation tool	

2. Project Terms

Customer Dependencies	In addition to any other responsibilities or assumptions described in this Agreement, the Customer Dependencies are as follows and the Customer recognises that if it fails to comply with the following dependencies, Vodafone is relieved from performing or delivering the Service and may choose to suspend or terminate this Agreement: • Customer shall perform and complete all responsibilities and assumptions set out in the Customer Prerequisites section prior to the Service Commencement Date. • the Customer will consent to and authorise Vodafone to access the required Customer Portal to configure, deploy and enable the Service. • Customer is solely responsible for: o Providing access to the Trend Micro Service Portal. o Providing access to mobile devices and accounts to be used to complete acceptance testing. o Ensure that the environment is fully functional and without issue before the integration work can take place.
General Assumptions & Dependencies	The general assumptions & dependencies applicable for this Service are: • All work is carried out on a fixed fee basis. • There will be no changes to the scope of the Service, as set out in this Agreement. • Vodafone may provide reasonable recommendations, advice or instructions on a particular course of action in the course of performing or as a result of the Service or in the Deliverables to be provided to Customer and if Customer chooses not to follow such reasonable recommendations, advice or instructions, Customer acknowledges that Vodafone shall not be responsible for any losses or claims made by the Customer that arise from Customer's failure to follow such recommendations, advice or instructions. • While Vodafone will use reasonable care to carry out the Service in line with Good Industry Practice and in a manner designed to mitigate and reduce the risk of damage to Customer Property, Customer acknowledges that there is inherent risk in the provision of the security Service in accordance with this Agreement which may lead to operational degradation, performance impact, breach of Customer policies or industry standards, or otherwise impair Customer Property (each a **"Customer Damage"** and together the **"Customer Damages"**) and, Vodafone will not be liable to the Customer or its respective employees or any third parties of the Customer for Customer Damages arising from the foregoing. To the extent possible, prior to commencing any provisioning of the Service, Vodafone shall identify and inform the Customer of any Customer Damage associated with the Service. • Customer agrees that Vodafone has the right to anonymise and aggregate Customer Data that will not in any way reveal the Customer Data as being attributable to the Customer with other data and leverage anonymous learnings and insights regarding use of the Service (the anonymised data, **"Vodafone Insights Data"**), and that Vodafone owns Vodafone Insights Data and may use Vodafone Insights Data during and after the term of this Agreement solely to develop, provide, and improve Vodafone products and services. • Customer agrees that Vodafone is not liable to Customer for Customer Damages provided that Vodafone will use reasonable care to carry out the Service in line with Good Industry Practice and in accordance with the terms of this Agreement. • The Customer agrees that, to the extent permitted by Applicable Law, it shall not bring any claim against Vodafone or any Group Company, whether in tort or otherwise, in connection with the Service or otherwise in relation to the subject matter of this Agreement. • Customer acknowledges that, in providing the Service, Vodafone will access Customer Systems and data. Customer agrees that, in advance of the

	Agreement Start Date, it shall provide and maintain all necessary consents, permissions, notices and authorisations that are necessary for Vodafone to perform the Service, including any of the foregoing from employees or third parties; valid consents from or notices to applicable data subjects; and authorisations from regulatory authorities, employee representative bodies or other applicable third parties (**“Customer Consent”**) in a timely manner as necessary for Vodafone to access and use such System and data to perform the Service under this Agreement, and/or to use any third-party System(s) or data that Vodafone may use or require access to in performing the Service. For the purposes of this Clause, **“System”** means, as applicable, Customer’s or a third party’s computer environment, network, equipment, software and related services. • Vodafone shall perform the Service in line with the scope of the Service as set out in this Agreement, in accordance with Good Industry Practice, and in reliance on, and in line with, the Customer Consent. • Customer agrees to indemnify Vodafone on an unlimited basis to the extent the Customer fails to provide and maintain the Customer Consents. • Vodafone is not responsible for remedying any security issues.
Materials and Software	• Vodafone is the ‘supplier’ of the Trend Micro services to its customers. • Trend Micro are the ‘partner’ who provide and host the service and are responsible for the maintenance, patching and up time of the service. • Customers will have full administration access to their own portal. • Customer support of the service is direct with Trend Micro.
Acceptance Testing	Acceptance testing will be completed by Vodafone Professional Services and the Customer as part of the delivery of the service. Acceptance testing will be considered complete when the Customer requirements detailed in advance have been met.
Out of scope statement	The following are not in scope for the Service: • any modification of environment settings other than those required to enable the Service. • Fault resolution of services other than Trend Micro. • End user communications. The services detailed in this SOW shall be provided remotely and constitute Vodafone’s complete scope of work and all other services (and the provision of services onsite) are out of scope.
Data Protection	1. Where Vodafone processes Personal Data, the relevant section of the clause headed “Data” of the Professional Services General Terms shall apply. 2. Vodafone may act as a Data Controller or Data Processor dependent upon the nature of the tasks undertaken as part of this Service. Vodafone acts as a Data Processor for the Processor Services only. 3. For the purposes of Clause 2 above, the “**Processor Services**” shall be defined as the activities in either of the following Deliverables where Vodafone Processes Personal Data as a Data Processor on behalf of the Customer as the Data Controller, in the direct performance of the delivery of the respective Deliverable(s) (where selected by the Customer): 1. Deliverable 1: Trend Micro configuration and deployment; and/or 2. Deliverable 2: Trend Micro Customer Integration. 4. For the avoidance of doubt, the definition of “Processor Service” shall not include Personal Data which is processed incidentally to the provision of the Service or the performance of Deliverable 1 or Deliverable 2. Such Personal Data shall be

	considered “Operational Data” for the purposes of the Professional Services General Terms. Where Customer shares Personal Data with Vodafone for the Processor Services, the Customer warrants and undertakes that it has complied with all necessary obligations imposed on it under Applicable Law including ensuring that it has either (i) obtained all necessary consents to transfer the Personal Data to Vodafone; or (ii) secured another lawful basis, in accordance with Applicable Privacy Law, to share such Personal Data with Vodafone for the processing envisaged by this Agreement and has provided appropriate privacy notices to the relevant data subjects (as required by Applicable Privacy Law) to enable it to share the Personal Data with Vodafone for the purposes envisaged by this Agreement

3. Standard Information

Contractual Terms	The Professional Services General Terms govern the relationship of the Parties in respect of the Service provided by Vodafone to the Customer under this SOW.
Minimum Term	Commencing on the Agreement Start Date and ending when the final Deliverable is provided by Vodafone to Customer. There shall be no Renewal Term.
Agreement Start Date	The date of the Customer's acceptance of the terms of this Agreement.

4. Charges

Charges	The Charges shall be set out in the Order and shall be exclusive of VAT at the prevailing rate.
Invoice	Charges shall be invoiced upon completion of the Service.

The following definitions are applicable to the Service, and are in addition to the definitions detailed in the Professional Services General Terms:

Customer Data	means all data, documents or records of whatever nature and in whatever form relating to the business of the Customer, the Customers' employees or otherwise, whether subsisting before or after the date of this Agreement and whether created or processed as part of, or in connection with, the Services.
Customer Property	means Endpoints, computer systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; confidential information; data (including Personal Data, employee identification, authentication or credential data user details and other sensitive information); assets; devices; intellectual property; and/or physical premises, that are used by Customer, or its respective employees, customers, or suppliers, whether owned or otherwise controlled by the Customer or owned by a third party.
Environment	means network connected devices such as servers, workstations, printers, scanners, phones, routers, switches, hypervisors, wireless devices and others. Environment does not include software applications.
External Infrastructure Penetration Test	means non-authenticated penetration testing which is performed against public facing infrastructure.
Good Industry Practice	means, in respect of any activity, performing that activity effectively, reliably and professionally in good faith and in a prompt and timely manner using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled, experienced and market leading operator engaged in the provision of the Service or such activity (as applicable) on a commercial basis.
Group Company	means Vodafone Group Company or a company or corporation within Vodafone Group (as the case may be).
Marketplace	means the platform set out at https://marketplace.vodafone.co.uk/home.
Service Commencement Date	the date as agreed between the parties for the Service to commence.
Virtual Machine	means the virtualisation/emulation of a computer system which is based on computer architectures and provides functionality of a physical computer.
Vodafone	means (a) Vodafone Limited, a company incorporated in England with registration number 1471587, whose registered office is at Vodafone House, The Connection, Newbury, Berkshire, RG14 2FN, England; and/or (b) a third party acting on behalf of Vodafone, which includes Accenture.
Worry Free Services	**means a Trend Micro Licence providing:** **Endpoint Security -**Secures Windows (desktops and servers), Mac, iOS, and Android devices by infusing high-fidelity machine learning into a blend of threat protection techniques for the broadest protection against ransomware and advanced attacks
Worry Free Services Advanced	**means a Trend Micro Licence providing:** **Endpoint Security -** Secures Windows (desktops and servers), Mac, iOS, and Android devices by infusing high-fidelity machine learning into a blend of threat protection techniques for the broadest protection against ransomware and advanced attacks **Email Security -** Secures Microsoft Exchange, Microsoft 365, Gmail and any other email solution in real time. Stops targeted attacks, spam, phishing, viruses, spyware, and inappropriate content from impacting your business. Includes our latest business email compromise and credential phishing protection capabilities **Collaboration Security -** Protects online collaboration tools from unknown threats and secures company data from intentional and accidental loss **Cloud App Security -**A cloud-based, advanced threat protection service that secures email and other cloud services in Office 365, Google Workspace™, Salesforce®, Box™, and Dropbox™.
Worry Free XDR	**means a Trend Micro Licence providing:** **Endpoint Security -** Secures Windows (desktops and servers), Mac, iOS, and Android devices by infusing high-fidelity machine learning into a blend of threat protection techniques for the broadest protection against ransomware and advanced attacks

	Email Security – Secures Microsoft Exchange, Microsoft 365, Gmail and any other email solution in real time. Stops targeted attacks, spam, phishing, viruses, spyware, and inappropriate content from impacting your business. Includes our latest business email compromise and credential phishing protection capabilities. Allows users to send and receive email during an email service outage **Collaboration Security -**Protects online collaboration tools from unknown threats and secures company data from intentional and accidental loss **Extended Detection and Response (XDR) -** Detection, response, and investigation capabilities within a single agent, across email and endpoints. Automated root cause analysis, including recommended step-by-step actions, allows quick mitigation. Advanced threat detection by cloud sandboxing included. Cross-customer detection, investigation, and response. (For MSPs only: do it yourself through Trend Micro Remote Manager) **Cloud App Security -** A cloud-based, advanced threat protection service that secures email and other cloud services in Office 365, Google Workspace™, Salesforce®, Box™, and Dropbox™.