

Service Specific Terms

Secure Access Gateway Service

Vodafone Business Customers



1. Term Commitment

1.1 Commercial Commitment:

- (a) Vodafone's offer is based on Customer using the Service for the Minimum Term.
- (b) The Order will set out the Minimum Term and the Service Type and at the expiry of the Minimum Term, Vodafone shall stop providing the Service and the Agreement shall terminate.

1.2 **Service Commencement Date:** The date that the Service is first provided by Vodafone under this Agreement.

1.3 **Renewal Term:** there shall be no Renewal Term

1.4 **Non-Recurring Charges:** One Off Charges may be billed from the Agreement Start Date, effective date as set out in the Order (or if not set out, then upon acceptance of the Order by Vodafone).

2. Charges

2.1 The Charges shall be as set out in the Order and shall be exclusive of VAT at the prevailing rate.

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

3. The Service – Overview

- 3.1 The Vodafone Business Secure Access Gateway service (the “**Secure Access Gateway**”) provides a user and application-centric approach to application access. A fully cloud-delivered service (in conjunction with our Applicable Vendors), Secure Access Gateway provides native application segmentation by using business policies to connect an authenticated user to an authorised application without bringing the user on the network.
- 3.2 Secure Access Gateway service will provision, manage and operate your cloud security control in a secured manner to protect Customer’s Environment from malicious activity in accordance with Customer’s security requirements. The term “Service” or “Services” in these Service Specific Terms means the Secure Access Gateway service.

4. Service Terms Structure

- 4.1 These Service Specific Terms include:
- (a) the service specification, which sets out a description of the Service, may be updated from time to time and is made available at www.vodafone.co.uk/cloudservices/ (the “**Service Specification**”);
 - (b) the service levels which set out the standards that will be applied to the provision of the Service (the “**Service Levels**”);
- 4.2 The following documents further govern Vodafone’s supply of the Service and form part of the Agreement:
- (a) the Commercial Terms;
 - (b) the Order, which sets out the Service Elements selected by/for Customer;
 - (c) the Vodafone Business Marketplace Service Specific Terms (the “**VBM Service Terms**”) available at www.vodafone.co.uk/cloudservices/;
 - (d) the General Terms available at www.vodafone.co.uk/terms;
 - (e) any other documents referenced as incorporated in these Service Specific Terms; and
 - (f) any applicable policies and guidelines, as provided from time to time by Vodafone.
- 4.3 These documents apply in the order of precedence set out in the General Terms, save that the VBM Service Terms shall take precedence over the General Terms and all documents expressed to be of lesser precedence in the General Terms.
- 4.4 **Zscaler End User Service Agreement (“EUSA”)**
- Customer acknowledges and agrees to abide by the EUSA. The Customer’s access and use of the Secure Access Gateway is subject to Customers acceptance of the EUSA. The latest version can be accessed from www.zscaler.com/legal.

5. The Service

- 5.1 The Customer must select one of the following types of Service (each a “**Service Type**”, together the “**Service Types**”):

Service Name	Description	Applicable Vendors
New Build	The provision and ongoing management of a new Secure Access Gateway instance to the Customer using the Applicable Vendors solutions.	<ul style="list-style-type: none">• Zscaler

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

Takeover	Takeover and ongoing management of the Customer's existing Secure Service Edge solution. Takeover applies to the Applicable Vendors existing Secure Service Edge only.	• Zscaler
-----------------	--	-----------

5.2 **Optional Service Elements:** In addition to the Service Type and Service Tier selected by Customer, the Customer may also select any of the following Optional Service Elements:

(a) **Pack of 10 Tickets:** additional pack of 10 Tickets provided where a Customer meets their Ticket quota (uses all of their Tickets).

5.3 The applicable Service Type and Optional Service Elements (if any) shall be set out in the Order and further detailed in the Service Specification.

6. Service Specific Conditions of Use

6.1 **Vodafone Business Marketplace** (the “VBM”): The Service is made available to purchase through the VBM. The VBM Service Terms apply to the extent of the Customer's use of the VBM website. In the event of any conflict between the VBM Service Terms and the Secure Access Gateway Service Terms, then the Secure Access Gateway Service Terms shall take precedence. 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.

6.2 Customer may use the Service only in accordance with the terms and obligations:

- (a) as indicated in the Order; and
- (b) as defined in the Agreement.

6.3 Vodafone shall only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the responsibilities set out in the Agreement, Vodafone's performance of the Service may be delayed, impaired or prevented.

6.4 **Adequate Customer Personnel:** Customer must provide adequate personnel to assist Vodafone in delivery of the Service, upon reasonable request by Vodafone.

6.5 **Delays:** delays due to infrastructure, access right unavailability or other underlying dependencies could result in additional efforts and costs and impact the duration and timelines of the Service.

6.6 **Termination:** In addition to the termination rights set out in the General Terms, Vodafone shall be entitled to terminate the Service upon 30 days written notice to Customer where Vodafone's agreement with the Third Party Provider has terminated.

6.7 **Payment Card Industry:** Vodafone does not warrant that the Service will be payment card industry (“PCI”) requirements Compliant or that the Services will enable Customer to be compliant with Applicable Privacy Law.

6.8 **Zscaler Provider Terms:**

(a) **Third-Party Products and Services:** Through its product(s), Zscaler may make available to Customer third-party products or services (“third-party apps”) which contain features designed to interoperate with its products. To use such features, Customer must either obtain access to such third-party apps from their respective providers or permit Zscaler to obtain access on Customer's behalf. All third-party apps are optional and if Customer chooses to utilise such third-party apps:

- (i) all governing terms and conditions, including licensing and, shall be entered into between Customer and the applicable app provider;
- (ii) Customer may be required to grant Zscaler access to its account on such third-party apps; and

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- (iii) Customer instructs Zscaler to allow the app provider to access Customer's data as required for the interoperation with the Zscaler products.
- (b) **Warranty:**
 - (i) With regard to any Zscaler products used in the provision of the Service, Vodafone warrants that:
 - (A) software shall substantially conform to the Zscaler Published Specifications for three (3) months from fulfilment. If Customer believes the warranty stated in this section has been breached, Customer must notify Zscaler of the breach no later than thirty (30) days following the date the warranty was allegedly breached, and if Zscaler determines that a defect exists, Zscaler will promptly correct the non-conformity at its own expense, and
 - (B) subscriptions shall perform materially to the Zscaler published specifications for the entire duration of the selected term.
 - (ii) As your sole and exclusive remedy and Zscaler's and its suppliers' sole and exclusive liability for breach of warranty, Zscaler shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable. All warranty claims must be made on or before the expiration of the warranty period specified herein, if any. Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Zscaler and replaced become the property of Zscaler. Zscaler shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Zscaler for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Zscaler. Zscaler will pay the shipping costs for repaired or replaced Products back to you
- (c) **Exclusions:** the warranty set forth above shall not apply if the failure of the Zscaler product results from or is otherwise attributable to:
 - (i) repair, maintenance or modification of the applicable Zscaler product by persons other than Zscaler or its designee;
 - (ii) accident, negligence, abuse or misuse of the applicable Zscaler product;
 - (iii) use of the applicable Zscaler product other than in accordance with the Zscaler Published Specifications and/or the EUSA;
 - (iv) improper installation or site preparation or Customer's failure to comply with environmental and storage requirements set forth in the Zscaler Published Specifications including, without limitation, temperature or humidity ranges; or
 - (v) causes external to the applicable Zscaler product such as, but not limited to, failure of electrical systems, fire or water damage.
- (d) **Disclaimers:** except for the warranties expressly stated and to the fullest extent permitted by Applicable Law, the Zscaler products are provided "as is". Vodafone and its Third Party Providers make no other warranties and expressly disclaim all other warranties, express or implied, including without limitation any implied warranties of merchantability, fitness for a particular purpose, and any warranties arising out of course of dealing or usage of trade. Vodafone and its Third Party Providers do not warrant that (i) the Zscaler products will meet Customer's requirements, (ii) the use of the Zscaler products will be uninterrupted or error-free, or (iii) the Zscaler products will protect against all possible threats whether known or unknown.

6.9 Customer Guidelines and Responsibilities. Customer agrees and understands that:

- (a) is responsible for all activity of Customer Users and it is responsible for Customer Users' compliance with this Agreement; it shall:

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- (i) have sole responsibility for the accuracy, quality, integrity, legality, reliability and appropriateness of all Customer data;
 - (ii) prevent unauthorized access to, or use of, the Products, and notify Vodafone promptly of any such unauthorized access or use; and
 - (b) the Products shall not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection, which shall be Customer's sole responsibility;
 - (c) in order for Vodafone and/or Third Party Provider to provide the SaaS, Customer is responsible for forwarding its web traffic to Vodafone and/or Third Party Provider via valid forwarding mechanisms that allow for automatic fail-over (i.e. PAC, IPSEC, GRE tunnels, and/or Software).
 - (d) it is responsible for supplying Vodafone and/or Third Party Provider with any technical data and other information Vodafone and/or Third Party Provider may reasonably request to allow Vodafone and/or Third Party Provider to provide the Products to Customer; and
 - (e) Vodafone and/or Third Party Provider shall have the right to
 - (i) use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Products
 - (ii) utilize the malware, spam, botnets, or other information related to the SaaS for the purposes of 1) maintaining, improving and/or analysing the SaaS, (2) complying with all legal or contractual requirements, and/or (3) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the SaaS; and
 - (iii) develop and commercialize benchmarks and measures based on Aggregated Data.
- 6.10 Further to Clause 7 of General Terms, Customer shall not, or allow a third party to;
- (a) access the Products in order to build a competitive product or service, or copy any ideas, features or graphics of the Products;
 - (b) use the Products to send spam or otherwise duplicative or unsolicited messages in violation of applicable laws;
 - (c) use the Products to send or store infringing, obscene, threatening, libellous, or otherwise unlawful or tortious material;
 - (d) use the Products to access blocked services in violation of applicable laws;
 - (e) upload to the Products or use the Products to send or store viruses, worms, time bombs, trojan horses or other harmful or malicious code, files, scripts, agents or programs.
 - (f) use the Products to run automated queries to web sites (as the web site may blacklist Third Party Provider IPs for all of its customers);
 - (g) interfere with or disrupt the integrity or performance of the Products or the data contained therein;
 - (h) attempt to gain unauthorized access to the Products or its related systems or networks;
 - (i) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Products;
 - (j) without the express prior written consent of the Third Party Provider, conduct any benchmarking or comparative study or analysis involving the Products ("benchmarking") for any reason or purpose except, to the limited extent absolutely necessary, to determine the suitability of Products to interoperate with Customer's internal systems.
 - (k) In addition, Customer agrees that it shall:
 - (i) use the Products solely for its internal business purposes; and

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- (ii) only permit access to the Products by Customer users.

6.11 Specific Terms for SaaS (Zscaler)

- (a) **Subscription Rights for Secure Internet Platform.** Subject to the terms and conditions set forth in this Agreement, the Customer is granted a limited, non-transferable/non-assignable (except as set forth in the Agreement), non-exclusive right to access and use the SaaS during the Term for the number of purchased authenticated Seats. A Seat may only be transferred from one individual to another if the original user is no longer permitted to access, and does not access, the Internet in connection with the SaaS.
- (b) **Subscription Rights for Guest Wi-Fi Security.** Subject to the terms and conditions set forth in this Agreement, the Customer is granted a limited, non-transferable/non-assignable (except as set forth in the Agreement), non-exclusive right to access and use the SaaS during the Term for the number of purchased Locations.
- (c) **Subscription Rights for Zscaler Private Access.** Subject to the terms and conditions set forth in this Agreement, the Customer is granted a limited, non-transferable/ non-assignable (except as set forth in the Agreement), non-exclusive right to access and use the SaaS during the Term for the number of purchased authenticated Seats. A Seat
 - (i) may only access and use the SaaS on up to two (2) devices (PDA, laptop, tablet, wireless phone, etc.) and
 - (ii) may only be transferred from one individual to another if the original user is no longer permitted to access, and does not access, the Internet in connection with the SaaS.
- (d) **Non-Authenticated Users for Secure Internet Platform.** In an environment where no user authentication is present, and only where Vodafone cannot reasonably determine the number of Seats being used by Customer, then every 2,000 Transactions per day flowing through the SaaS shall be considered a "Seat" (i.e. the number of Seats used would be calculated by dividing the total number of Transactions flowing through the SaaS per day by 2,000)
- (e) **Customer Transaction Logs for Guest Wi-Fi Security.** Vodafone will not access, read or copy any Customer Data other than by electronic methods and solely for the purposes of providing services to Customer under this Agreement and the Order. In order to provide the SaaS under this Agreement, Customer agrees that Vodafone shall have the right to use, reproduce, store, modify, and display the information from Customer's Raw Transaction Logs (i.e. the metadata of all network traffic sent to or received from Customer through its use of the Services) and Customer's Summarized Transaction Logs (i.e. the summarized versions of the Raw Transactions Logs) (collectively the "Customer Transaction Logs"). Customer's Raw Transaction Logs shall be retained by Vodafone for rolling two (2) week periods during the Term, and Customer's Summarized Transaction Logs shall be retained by Vodafone for rolling six (6) month periods during the Term. Upon expiration of the Term, all Customer Transaction Logs shall be deleted by Vodafone pursuant to the two (2) week or six (6) month retention cycles or as earlier requested in writing by Customer. If Customer orders the Nanolog Streaming Service (NSS), then Customer shall be able to stream the Customer Transaction Logs in real-time to Customer's premises and systems allowing Customer to retain the Customer Transaction Logs for however long it chooses.
- (f) **Customer Transaction Logs for Secure Internet Platform and Zscaler Private Access.** Vodafone will not access, read or copy any Customer Data other than by electronic methods and solely for the purposes of providing services to Customer under this Agreement and the Order. In order to provide the SaaS under this Agreement, Customer agrees that Vodafone shall have the right to use, reproduce, store, modify, and display the information from Customer's transaction logs (i.e. the metadata of all network traffic sent to or received from Customer through its use of the Services) (hereinafter the "**Customer Transaction Logs**"). Customer Transaction Logs shall be retained by Vodafone for rolling six (6) month periods during the Term. Upon expiration of the Term, all Customer Transaction Logs shall be deleted by Vodafone pursuant to the six (6) month retention cycles or as earlier requested in writing by Customer. If

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

Customer orders the Nanolog Streaming Service (NSS), then Customer is able to stream the Customer Transaction Logs in real-time to Customer's premises where the Customer Transaction Logs can be sent to multiple Customer systems allowing Customer to retain the Customer Transaction Logs for however long it chooses.

- (g) **Excessive Bandwidth Consumption for Secure Internet Platform and Zscaler Private Access.** If Customer's average per-Seat bandwidth consumption increases above Customer's Bandwidth Baseline by more than one-hundred percent (100%) for a sustained ninety (90) day period, Vodafone will notify Customer and Customer agrees to work with Vodafone in good faith on a bandwidth reduction plan, or to work with Vodafone in good faith to renegotiate pricing for the remainder of the Term. If the parties are unable to reach a mutually agreeable solution within thirty (30) days, then Vodafone may, upon thirty (30) days' written notice, terminate the remaining portion of the Term and refund to Customer any prepaid Fees pro-rated for the unused portion of the Term. For purposes of this Agreement, "Customer's Bandwidth Baseline" means the average per-Seat bandwidth consumption determined by Vodafone over the 90-day period following the start of Customer's subscription to the SaaS.
- (h) **Additional Seats or Locations (applicable for all SaaS).** For any additional Seats or Locations needed during the Term, Customer agrees to place an additional Order with Vodafone for such additional Seats or Locations. Any such agreement will be reflected in a new Order. If Vodafone determines that Customer is using more Seats or Locations than it has purchased, Customer agrees that Vodafone may invoice Customer for the additional Seats or Locations as per the new Order.

6.12 Specific Terms for software (Zscaler)

- (a) **Scope of License.** On satisfaction of the Customer's payment obligations, the Customer shall be granted a limited, non-transferable/non-assignable (except as set forth in this Agreement), non-exclusive sublicense in respect of the Product and Vodafone hereby acknowledges and agrees that it has been provided all necessary consents from third-parties in order for the same to occur.
- (b) **Personal Data/UDID.** Customer agrees and understands that the Software will be used by Customer in combination with SaaS in order to transmit from and receive certain data in Customer's mobile device or portable (laptop or desktop) computer. Such data may include location-based information that tracks Customer's whereabouts and that are contained in unique device identifiers (UDID) that Customer stores or receives on or sends from its mobile device or portable (laptop or desktop) computer ("Personal Data"). Customer expressly consents to Vodafone's collection, storage, and processing of such Personal Data pursuant to the terms and conditions in this Agreement.

7. Deliverables

- 7.1 The Deliverables are set out in the Service Specification.
- 7.2 Vodafone will use secure methods of transmission of the Deliverables to the Customer. If the Customer requires a specific technology to be used, the Customer is responsible for providing Vodafone with access to the technology for transmission.
- 7.3 The Deliverables are provided only for the Customer and the Customer may be permitted to disclose the Deliverables to its respective affiliates, directors, and employees.
- 7.4 The Deliverables are intended for Customer's own internal use only and not for any use by third parties nor for use in any legal proceedings. Vodafone disclaims any liability that may arise out of any third-party's review and/or use of such Deliverables, or arising out of, or in connection with, such Deliverables being used in legal proceedings. In no circumstances will Vodafone be required to provide expert testimony in connection with the provision of the Service or any Deliverables under this Schedule.
- 7.5 Customer agrees that it is responsible for:

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- (a) assessing the applicability to Customer's business and operations of the Deliverables and the Service, and any recommendations, advice or instructions provided by Vodafone in the course of providing the Service; and
- (b) determining whether the Service and Deliverables provided by Vodafone, including any revised business processes implemented pursuant to each applicable Order:
 - (i) meet Customer's business requirements;
 - (ii) comply with all Applicable Laws; and
 - (iii) comply with Customer's applicable internal guidelines, long-term goals and any related agreements.

8. General Assumptions and Dependencies

- 8.1 There will be no changes to the scope of the Service set out in these Service Specific Terms.
- 8.2 The Customer point of contact will be accountable for identifying the stakeholders within the Customer environment relevant to the Service.
- 8.3 Customer is responsible for the remediation and resolution of security events (in their computer systems) and incident tickets.
- 8.4 Customer computer systems that are within scope of the Secure Access Gateway service are without defect.
- 8.5 In order to receive the Secure Access Gateway service, Customer must have a platform from the Applicable Vendor list with required access for Vodafone and rights to use with 24x7 availability.
- 8.6 Required connectivity and access, provided by Customer, will be in place before the Secure Access Gateway service commences. Customer will ensure all infrastructure, access rights and other underlying dependencies are in place in timelines that support the project delivery unless mutually agreed in writing. Additional effort, costs and impact to the duration and timelines of the project may occur if this is not in place.
- 8.7 Customer will provide their own support for connectivity with own devices/infrastructure.
- 8.8 **New Build Service:** where Customer does not have an existing Applicable Vendor technology, Customer agrees to procure this technology from Vodafone as part of the order. Customer will provide all third party necessary consents, permissions, notices and authorisations as that are necessary for Vodafone and our delivery partners to access the Applicable Vendor technology in order to perform the Secure Access Gateway service ("**New Build Service**").
- 8.9 Where Customer has selected the New Build Service type, if the Customer requests one of the following activities, the Customer shall provide the necessary trusted certificates:
 - (a) the logs stored in the Zscaler tenant to be forwarded to Customer's syslog or security operations centre ("**SOC**") solution.
 - (b) Customer is responsible for providing and maintaining the applicable certificates required for the Service. Customer must provide the required certificates and assumes all responsibility for the decryption of the SSL traffic.
- 8.10 **Takeover Service:** Where Customer selects the Takeover Service Type, communication during the Customer Site survey and installation phase will be in English. Vodafone shall provide all documentation in English.
- 8.11 Standard design templates will be used for all deliverables where possible, including reporting, the Operating Manual and the Escalation Matrix. Where Customer requirement is complex in nature and/or requires a non-standard approach we may decide it is possible to support Customer requirements which may be subject to a separate charge, to be agreed with Customer and set out in a separate contract.

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- 8.12 Customer will provide Vodafone with detailed requirements for the Secure Access Gateway service in the Scoping Template. Vodafone will help Customer to obtain such detailed requirements where possible. Vodafone require the Scoping Template to be completed in full before we can create the project scoping documentation during the Establish Context phase of the Initial Setup and Build.
- 8.13 Zscaler tenant access will be in place before Vodafone start deploying Customer Secure Access Gateway service.
- 8.14 Customer will perform all the necessary changes to their environment that are needed for the integrations defined in the LLD. Customer will provision the required on-premises devices (where applicable and where defined in the LLD).
- 8.15 Local agent software will be owned, deployed and managed by Customer.
- 8.16 Customer will receive your SOC services from a shared SOC team i.e. Customer will not have a dedicated SOC team working exclusively on the Secure Access Gateway service.
- 8.17 The Service does not provide monitoring of Security Events, any Security Event mitigation or advice regarding security issues or threats outside of the Service.
- 8.18 Customer must promptly notify Vodafone of any changes to information, provided by Customer to Vodafone, in relation to the Service.
- 8.19 Customer shall:
 - (a) provide to Vodafone the High-level design for each of the Customer Sites where the Service needs to be deployed before commencement of the Low-Level Design phase; and
 - (b) respond to Vodafone inputs and requests in time (within 1 Working Day of receipt) to ensure the project is completed as per the planned schedule.
- 8.20 Customer agrees it is responsible for the connectivity of and between its networks and for providing appropriate bandwidth to avoid packet drops or loss of communications, unless otherwise mutually agreed by Vodafone and Customer in writing.
- 8.21 Customer, on behalf of itself and its third-party licensors, consents, authorises and grants to Vodafone the right to access the Customer's Environment and the right to retrieve data stored in or produced by the Customer's Environment in order to provide the Service. Customer agrees that if the Customer upgrades or otherwise changes the Customer's Environment, Customer will work with Vodafone in good faith to determine the impact to the Service.
- 8.22 Customer agrees that where it provides its approval this means that it has followed its own internal approval requirements and Vodafone can rely on such approval and is not required to confirm/check any such approval. Where Customer is requested to sign off on key decisions and deliverables, Customer will be accountable for this and will provide it within 3 working days.
- 8.23 Customer acknowledges that it has knowledge and skill particular to its business practices and it will share such knowledge and skill and provide Vodafone with access to Customer subject matter resources, to facilitate the provision of the Service and Deliverables.
- 8.24 Subject to Vodafone's approval, where Customer has selected the Takeover Service Type and Customer requests additions and/or changes to its existing Zscaler solution (e.g. additional controls / users / applications, incidents, changes, etc), these will be subject to a separate charge and agreement, to be agreed with the Customer.
- 8.25 Customer will manage their Applicable Vendors and facilitate coordination between such Applicable Vendors and Vodafone.

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- 8.26 Customer will arrange any calls or meetings required (using Vodafone approved industry-standard collaboration tools, such as Microsoft Teams, or other industry-standard collaboration technology) when requesting that Vodafone provide level 2 Support following notification of an incident.

9. Security Requirements

- 9.1 Customer agrees it retains full responsibility for: (i) ensuring that the security requirements comply with all applicable laws, industry self-regulatory codes, meet Customer's business requirements, and comply with Customer's applicable internal guidelines, long-term goals, and any related agreements; (ii) pursuing any enforcement or legal action with regard to such requirements; and (iii) reviewing and updating the security requirements to reflect technological developments. Nothing in this Agreement shall be interpreted to mean that Vodafone verifies that such security requirements comply with applicable laws, Customer's internal guidelines, and related agreements, or otherwise meet Customer's business requirements.
- 9.2 Compliance with Customer security policies shall not require Vodafone to provide any service beyond the scope of this Schedule.
- 9.3 Customer will not be entitled to make a claim against Vodafone for losses suffered or incurred by Customer to the extent such losses are the result of a security defect that: (i) exists in the Customer's legacy environment; or (ii) is introduced into the Customer's legacy environment by Customer or a third-party provided that such claim or loss is not attributable to or caused by: a) Vodafone negligence; or b) a Vodafone failure to perform the Services in line with terms of this Agreement.

10. Data Protection

- 10.1 Where the 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.
- 10.2 For elements of this Service, Vodafone may act in the capacity as a Data Processor ("**Processor Services**").
- 10.3 Vodafone (and its subcontractors):
- (a) may Process User Personal Data for: (i) provision and monitoring of the Service; or (ii) any other purpose agreed between the parties subject to Customer's prior written consent. Additional instructions require prior written agreement and may be subject to Charges. Customer shall ensure that its instructions comply with Applicable Laws.
 - (b) may use User Personal Data to create statistical data and information about service usage and devices that does not identify a User.
 - (c) may engage another processor (a "**Sub-Processor**") to carry out processing activities in the provision of the Services or to fulfil certain obligations of Vodafone under the Agreement. Vodafone shall inform the Customer of changes to Sub-Processors where Vodafone is required by Applicable Privacy Law by (i) providing at least ten (10) Working Days' prior notice, or (ii) listing the new or replacement Sub-Processor on www.vodafone.co.uk and/or at least ten (10) Working Days before Vodafone authorises and permits the new or replacement Sub-Processor access to User Personal Data in order to give the Customer the opportunity to reasonably object to such changes. Vodafone will enter into a contract or other legal act with the Sub-Processor and will impose upon the Sub-Processor substantially the same legal obligations as under this clause to the extent required by Applicable Privacy Law and that the Sub-Processor is carrying out the relevant processing activities. Vodafone shall remain liable to the Customer for the performance of that Sub-Processor's obligations.

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- (d) may retain the User Personal Data for as long as is required to deliver the Service and shall destroy or return (at Customer's option) User Personal Data in its possession upon termination of the Agreement, save where Customer opts for Vodafone to retain User Personal Data subject to a new hosting agreement.
 - (e) shall limit access to User Personal Data to those necessary to meet Vodafone's obligations in relation to the Service and take reasonable steps to ensure that they: (i) are under an appropriate statutory obligation of confidentiality; (ii) are trained in Vodafone's policies relating to handling User Personal Data; and (iii) do not process User Personal Data except in accordance with the Customer's instructions unless required to do so by Applicable Law.
 - (f) shall (i) provide appropriate technical and organizational measures for a level of security appropriate to the risks that are presented by Processing; and (ii) comply with the security requirements contained in the Vodafone information security policies and/or based on ISO 27001;
 - (g) shall (i) provide Customer with such information, assistance and co-operation as Customer may reasonably require to establish compliance with Applicable Privacy Law including any personal data breach notification; (ii) without undue delay, notify Customer of any unauthorised access to User Personal Data of which Vodafone becomes aware, which results in loss, unauthorised disclosure or alteration to the User Personal Data; and (iii) where required by Applicable Privacy Law and requested by the Customer (prior to the processing), provide the Customer reasonable assistance to carry out a privacy impact assessment of the Services and any prior consultation of the relevant supervisory authority.
- 10.4 **Audit:** Customer shall with respect to any right of audit, including inspections, which they may have under Applicable Privacy Law relating to data protection, agree to exercise such right as follows: (a) no more than once per annum following the Agreement Start Date, request to meet (on a mutually acceptable date) with one or more senior representatives of Vodafone's security and/or audit department to review Vodafone's security organization and the best practice and industry standards which Vodafone meets or to which it aspires, including, without limitation, ISO 27001 (or equivalent), provided that such audit shall relate to the Services only. If the Transfer Contract Clauses apply (the model contract clauses set out in the European Commission's Decision 2021/914 dated 4 June 2021 for transfers of Personal Data to countries not otherwise recognised as offering an adequate level of protection for Personal Data to countries not otherwise recognised as offering an adequate level of protection for Personal Data by the European Commission, as may be amended or replaced by the European Commission from time to time ("EU Transfer Contract Clauses") and the UK Transfer Contract Clauses collectively, as amended, replaced and complemented from time to time by the UK's Information Commissioner Office ("UK Transfer Contract Clauses")), nothing in this clause 8.4 amends or varies those standard clauses nor affects any data subject or supervisory authority's rights under those clauses; and (b) be responsible for reviewing the information made available by Vodafone and making an independent determination if the Services meet the Customer's requirements and legal obligations as well as its obligations under this clause.
- 10.5 **Transfer of User Personal Data out of the UK and the European Economic Area ("EEA"):** Vodafone may transfer User Personal Data to countries outside the UK and the EEA that have not been designated by the European Commission or Secretary of State in the UK as ensuring an adequate level of protection under Applicable Privacy Law, only to the extent that (i) User Personal Data is transferred on terms substantially in accordance with the Transfer Contract Clauses for the transfer of Personal Data to processors established in third countries; (ii) that the transfer of User Personal Data does not put any member of Customer Group in breach of its obligations under Applicable Privacy Law; or (iii) it is required to do so by Union or Member State law to which it is subject; in such a case, Vodafone shall inform the Customer of that legal requirement before processing, unless that law prohibits such information.
- 10.6 **Law enforcement authorities:** Vodafone: (i) may receive legally binding demands from a law enforcement authority for the disclosure of, or other assistance in respect of, User Personal Data, or be required by Applicable Law to disclose User Personal Data to persons other than Customer; (ii) will not be in breach of its obligation to Customer in complying with such obligations to the extent legally bound; and (iii) shall notify Customer as soon as reasonably possible of any such demand unless otherwise prohibited.

Service Specific Terms

Secure Access Gateway Service



Vodafone Business Customers

- 10.7 **Enquiries from Users:** Vodafone shall, where the Customer is required under Applicable Privacy Law to respond to enquiries or communications (including subject access requests) from Users and taking into account the nature of the processing (i) without undue delay pass on to Customer any enquiries or communications (including subject access requests) that Vodafone receives from Users relating to their User Personal Data or its Processing; and (ii) assist the Customer by appropriate technical and organizational measures, insofar as this is possible in the Customer's fulfilment of those obligations under Applicable Privacy Law

11. Delivery

- 11.1 Vodafone will make the Service available to Customer on the Service Commencement Date.
- 11.2 The Service shall be provided from the UK and India in English language.

12. Out of Scope Activity

- 12.1 Anything not specifically described in these Service Specific Terms is out of scope and is not included in the Service. In addition, and for avoidance of doubt, the following are not in scope for the Service:
- (a) any physical onsite support in Customer locations, where applicable;
 - (b) configuration of switches and other network devices;
 - (c) Configuration of security devices not related to Vodafone Business Secure Access Gateway service
 - (d) UAT and product training to Customer. While Vodafone will perform service-readiness testing during the Initial Setup and Build, UAT is out of scope and will be performed by Customer if needed. However, Vodafone will provide support for a period of up to 48 hours after the service has transitioned into a live state;
 - (e) ownership and maintenance of computer systems which are used by Customer in your environment to protect or host any components of the Applicable Vendor solution;
 - (f) procurement of solution components;
 - (g) fixing product related bugs on the Applicable Vendor solution. This remains the responsibility of the Applicable Vendor and will be carried out by the Applicable Vendor on their cloud hosted SaaS platform;
 - (h) providing a separate SIEM / log management solution;
 - (i) fine-tuning and support of controls, systems that have not been onboarded under the Secure Access Gateway service;
 - (j) technical remediation or resolution of an incident in Customer network environment related to alerts generated by the Secure Access Gateway service. Vodafone shall effect changes where applicable on the Secure Access Gateway service where this is required, however it shall be Customer responsibility to carry out remediation or resolution of issues in their environment.
 - (k) deployment and management of software agent in Customer environment.

Service Levels

Secure Access Gateway service



Vodafone Business Customers

13. Service Levels

For the avoidance of doubt;

- Availability SLA's of the Secure Access Gateway service are dependent upon availability of the Applicable Vendor SaaS.

13.1 Zscaler service availability is stated as $\geq 99.999\%$ except for Excluded Applications (see <https://www.zscaler.com/legal/sla-support>). The Standard Service Levels are as follows:

Priority	Reactive response time	Resolution time (reactive or proactive)
1	30 minutes	4 hours
2	60 minutes	8 hours
3	24 hours	72 hours

- (a) Availability SLA's of the Secure Access Gateway service are dependent upon availability of the Applicable Vendor SaaS.
- (b) Zscaler service availability is stated as $\geq 99.999\%$ except for Excluded Applications (see <https://www.zscaler.com/legal/sla-support>).
- (c) Service Levels as described above will not apply during the maintenance windows, third party dependency or any downtime Incident Management.

13.2 Measurement of Service Levels

- Incident Response and Incident Resolution SLA's will not apply until 30 days after the completion of Initial Set up and Build.
- SLA will be measured on a monthly basis.
- A minimum threshold of 95% applies to the SLA, in other words if 95% or greater of incidents meet the SLA then the SLA will deemed to have been met.

The following sets out the manner in which the Service Level Value for each of the Service Levels referred to in the table above will be calculated.

- (a) SLA 1: Incident Response Time for Priority 1

$$\text{SLA 1} = A / B * 100\%$$

where:

- A** means the number of Priority 1 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 30 minutes or less
- B** means the total number of Priority 1 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

- (b) SLA 2: Incident Response Time for Priority 2

$$\text{SLA 2} = C / D * 100\%$$

Service Levels

Secure Access Gateway service

Vodafone Business Customers



where:

- C** means the number of Priority 2 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 60 minutes or less
- D** means the total number of Priority 2 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

- (c) **SLA 3** **Error! Reference source not found.:** Incident Response Time for Priority 3

$$SLA\ 3 = E / F * 100\%$$

where:

- E** means the number of Priority 3 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 1 Working Day or less
- F** means the total number of Priority 3 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

- (d) **SLA 4:** Incident Resolution Time for Priority 1

$$SLA\ 4 = G / H * 100\%$$

where:

- G** means the number of Priority 1 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 4 hours or less
- H** means the total number of Priority 1 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

- (e) **SLA 5:** Incident Resolution Time for Priority 2

$$SLA\ 5 = I / J * 100\%$$

where:

- I** means the number of Priority 2 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 8 hours or less
- J** means the total number of Priority 2 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

- (f) **SLA 6:** Incident Resolution Time for Priority 3

$$SLA\ 6 = K / L * 100\%$$

where:

- K** means the number of Priority 3 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 3 Working Days or less

Service Levels

Secure Access Gateway service



Vodafone Business Customers

- L** means the total number of Priority 3 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

14. Dependencies

The following sets out the Dependencies for each of the Service Levels referred to in Clause 13 (Service Levels).

14.1 Customer Dependencies

- (a) The Customer Dependencies applicable to all Service Levels referred to in Clause 0 (Service Levels) are as follows.
- (i) Vodafone can remotely access the Customer's systems with rights to use with 24x7 availability.
 - (ii) The Customer's subject matter expert is available for testing.
 - (iii) The Customer has OEM contracts and premier support in place for hardware and parts replacement.
- (b) SLA 4: Incident Resolution Time for Priority 1: The additional Customer Dependencies for SLA 4 are as follows.
- (i) Downtime of the Customer's systems is provided (for a period directed as by Vodafone) for Incident resolution.
- (c) SLA 5: Incident Resolution Time for Priority 2: The additional Customer Dependencies for SLA 5 are as follows.
- (i) Downtime of the Customer's systems is provided (for a period directed as by Vodafone) for Incident resolution.
- (d) SLA 6: Incident Resolution Time for Priority 3: The additional Customer Dependencies for SLA 6 are as follows.
- (i) Downtime of the Customer's systems is provided (for a period agreed with the Customer) for Incident resolution.

15. Incident Priority Levels and Definitions

- 15.1 Below is the "**Incident Priority Impact**" matrix which sets out the scoring used to determine the Priority of an Incident between Priorities 1, 2, 3, and 4, such matrix which is aligned to the ITIL framework.
- 15.2 Each Incident will be assessed in terms of its impact upon the business with which the business requires the Incident to be resolved or a work around to be implemented, by applying the below matrix. The Incident shall be assigned a Priority based on this assessment.

Table 1: Incident Priority Impact Matrix

Priority Level	Impact			
	1 – Critical / Major	2 – Significant	3 – Moderate	4 – Minor

The definitions of impact for assessing priority level with respect to the overall Customer base and the individual Customer are detailed below:

Service Levels

Secure Access Gateway service

Vodafone Business Customers





Priority level	Priority level description
1	Critical or major: An Incident that results in a critical business impact to Customer, assigned where (i) Customer experiences a complete or substantial loss of Customer System, (ii) a mission critical business process is not working, (iii) where no delay for resolution is accepted (impact on Customer System or is causing revenue leakage), (iv) total loss of one or more Customer Systems that results in the Customer Systems being unavailable, or (v) security vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.
2	Significant: An Incident that results in some business impact, assigned where (i) a defect results in a critical business impact, but can be circumvented, (ii) certain functions within the software are disabled, but the business process remains operable, (iii) degradation of Customer Systems. Example: Intermittent fault or substantial degradation of one or more of the Customer Systems that substantially impacts the Customer System, or iv) there are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.
3	Moderate: An Incident that results in a minimal business impact, assigned where (i) Customer experiences no loss of Customer Systems and the Incident has no significant effect on the usability of the infrastructure, (ii) the Incident materially affects the use of the Customer Systems, that is not a Priority 1 or 2 Incident such as a loss of a second site, failure of one or more resilient items of Customer Systems, failure of a feature of non-resilient Customer Systems e.g. power supply failure in a server, or (iii) the potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.
4	Minor: All other Incidents that do not materially affect the use of the Customer Systems not covered within the above (low impact on business and less urgency on fixing the Incident), or no unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.



Secure Access Gateway Service

Vodafone Business Customers

Appendix A - Ticket Management

Service Requests

The following are standard service requests that can be raised by Customers:

Product	Category	Subcategory	Category Type	Debited from quota
Secure Access Gateway	Inquiry	General	Request (Normal Change)	Not debited
Secure Access Gateway	Account	Password Reset	Request (Standard Change)	Not debited
Secure Access Gateway	Account	Create	Request (Standard Change)	Not debited
Secure Access Gateway	Configuration	PAC file	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	Client connector upgrade	Request (Standard Change)	Debited
Secure Access Gateway	Configuration	Security policy	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	Provisioning of new application	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	SAML authentication	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	Posture profile configuration	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	Application modification	Request (Normal Change)	Debited
Secure Access Gateway	Configuration	URL Categorization	Request (Standard Change)	Debited
Secure Access Gateway	Configuration	URL IP Deny List	Request (Standard Change)	Debited
Secure Access Gateway	Configuration	URL Whitelisting	Request (Standard Change)	Debited
Secure Access Gateway	Configuration	URL recategorization	Request (Standard Change)	Debited
Secure Access Gateway	Configuration	URL Allow List	Request (Standard Change)	Debited



Secure Access Gateway Service

Vodafone Business Customers

16. Definitions

16.1 The following definitions are applicable to the Service

Applicable Programming Interface or API	means Applicable Programming Interface which allows different computer systems to communicate and exchange information in an automated manner.
Applicable Vendors	means those vendors listed in clause 5.1.
Change Request	means addition, modification, or removal of anything that could have a direct or indirect effect on services to IT infrastructure, applications or any other critical component.
Customer Data	means all Personal Data or information submitted by or on behalf of Customer to the Products.
Customer Users	means employees, agents, guests (for Guest Wi-Fi Security only) and other third parties authorized by Customer to download, deploy, access, install, or use the Products.
Custom Reporting	means the creation of customised operational report(s) within the NGFW to suit the pre-determined requirements of the Customer and to the extend technically and reasonably possible by the NGFW product. (e.g., customised reports).
Data Packet	means a unit of data made into a single Internet Protocol (IP) package that travels along a given network path.
Deliverables	means any deliverable, process or document to be provided by Vodafone in accordance with these Service Terms and as detailed in the Service Specification.
DNS Transaction	means a recursive DNS query sent from Customer through its use of the SaaS.
Documentation	means the user manuals generally provided in writing to end users of the Products in electronic format, as amended from time to time.
Environment	means the Customer's relevant systems, security controls, network infrastructure, and Endpoints.
Excluded Transactions and Sessions	means Transactions and Sessions that are not processed due to (a) failure by Customer's network to forward traffic to Third Party Provider; (b) failure by an intermediate ISP (other than Third Party Provider's direct ISP(s)) to deliver traffic to Third Party Provider; and/or (c) a Customer-implemented policy change that causes Transactions and Sessions to drop.
Generic Routing Encapsulation or GRE	means Generic Routing Encapsulation, which is a protocol for encapsulating data packets in order to set up a direct network connection.
Group Company	means an or a company or corporation within Vodafone Group (as the case may be).



Secure Access Gateway Service

Vodafone Business Customers

Incident	means an event which causes, or may cause, an unplanned interruption to the Service or a reduction in the quality of the Service.
Incident Resolution Time	means the period commencing at the time (rounded up to the next whole minute) at which the Incident Ticket in respect of an Incident has been Responded To and ending at the time (rounded down to the previous whole minute) that such Incident is Resolved.
Incident Response Time	means the period commencing at the time (rounded up to the next whole minute) at which Vodafone receives an Incident Ticket and ending at the time (rounded down to the previous whole minute) at which the Incident Ticket has been Responded To.
Incident Ticket	means a request issued by Customer to Vodafone via phone in relation to an Incident.
IPSec	means a suite of related protocols that tunnel data between devices and cryptographically secure communications at the network layer.
Known Virus	means a virus for which, at the time of receipt of content by Third Party Provider: (i) a signature has already been made publicly available for a minimum of one (1) hour for configuration by Third Party Provider's third party commercial scanner; and (ii) is included in the Wild List located at http://www.wildlist.org and identified as being "In the Wild" by a minimum of three (3) Wild List participants.
Location	means a subscription for a specific access point to the Internet in connection with the SaaS.
Materials	means all proprietary materials, Intellectual Property Rights for all Products and Documentation, processes and methods, and/or materials distributed during any presentations, proof of concepts, or demonstrations of Products.
LLD	means Low Level Design which is a component-level design process that follows a step-by-step refinement process.
Network address Translation or NAT	means Network Address Translation, a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
Order	means a written order form, purchase order or similar ordering document for Products submitted to Third Party Provider by Vodafone.
PAC or Proxy Auto-Configuration	means Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browser requests go direct to the destination or are forwarded to a web proxy server (Zscaler).
Premium Data Centre	means the deployment and use of the SaaS by a Customer in a region or country that requires a bandwidth surcharge as defined in the Price Book. For purposes of clarity, these premium regions are Australia, Mainland China, the Middle East, South America and South Africa.



Secure Access Gateway Service

Vodafone Business Customers

Priority	means, in respect of an Incident, the Priority level of such Incident as determined in accordance with the Service Levels.
Products	means, collectively, all Third Party Provider SaaS, Software, and Hardware.
Professional Services	means the professional services provided to Customer as set forth in a Statement of Work.
Qualified DNS Transactions	means the following: (i) the lookup is already cached by Third Party Provider's recursive DNS server, or if it's not cached, the response time of the authoritative DNS server is not counted as part of the Latency Agreement; and (ii) a reasonable level of service consumption (based on the number of purchased DNS Transactions per Location).
Qualified Transactions and Data Packets	means the following: (i) less than 1 MB HTTP GET request and response; (ii) not SSL-intercepted; (iii) not related to streaming applications; (iv) not subject to bandwidth management rules (QoS enforcement); and (v) a reasonable number of Transactions and Data Packets per Seat (based on Third Party Provider's cloud wide average).
Resolved	means, in respect of an Incident, its Incident Ticket has been resolved by Vodafone.
Responded To	means, in respect of an Incident Ticket, Vodafone communicates to the Customer that its Incident Ticket has been received.
Scoping Template	means a form which is completed by the Customer (with assistance from Vodafone Business if needed) which details the Customer's requirements in relation to the service. This will include any Add-ons that are required.
Seat	means a subscription for a specific individual user that accesses the Internet in connection with the SaaS.
Security Assertion Markup Language or SAML	means Security Assertion Markup Language, an open standard for exchanging authentication and authorisation data between parties (for example between an identity provider and a service provider) .
Security Event	means any act or attempt by people or malicious software to gain unauthorized access, disrupt service, or use systems or data in violation of Customer's policies.
Service Level(s)	the service levels that apply to the provision of the Service as set out in these Service Terms.
Service Request or SR	means the service requests listed in Appendix A raised from a User or on behalf of a User that initiates a service action as a part of normal service delivery. Service Requests cannot be used in response to a failure or degradation of services.
Security Information and Event Management or SIEM	means Security Information and Event Management (SIEM for short), which is a solution that helps organizations detect, analyse, and respond to security threats before they harm business operations.



Secure Access Gateway Service

Vodafone Business Customers

	SIEM, pronounced “sim,” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.
Secaure Service Edge or SSE	means a technology from Applicable Vendor which secures access to the web, cloud services and private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service, and may include on-premises or agent-based components.
Session	means any non-HTTP or HTTP request sent to or from Customer through its use of the SaaS.
Software	means any software, utility, tool or other computer or program code, in object (binary) or source-code form provided, directly or indirectly to Customer as well as to any copies (whether complete or partial) made by or on Customer’s behalf, as further detailed in Exhibit B. The term “Software” also includes any updates, upgrades or other new features, functionality or enhancements to the Software made available directly or indirectly to Customer.
Software as a Service or SaaS	means a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers
Statement of Work or SOW	means the document agreed by the parties setting out as applicable the services and documentation to be provided by supplier under the terms of this agreement.
SSL	means Secure Sockets Layer, a standard protocol used to establish a secure communication connection between two devices (for example between a server and a client). A protocol which has been deprecated and replaced by a newer protocol Transport Layer Security (TLS).
Tenant	Means a virtual firewall, hosted by Palo Alto. A dedicated tenant is for a single customer. A shared tenant is between two or more Customers.
Third Party Provider	a third party contracted directly or indirectly by either Vodafone (including Vodafone Group) or Customer that provides a Service, a Third Party Service or that provides a service that connects to a Service. Third Party Providers may include incumbent providers.
Ticket	means a request issued by a Customer to Vodafone in relation to Incident management, Service Request management or Change Request management.
Transaction	means an HTTP or HTTPS request sent to or from Customer through its use of the SaaS.
UAT	means User Acceptance Tests.
Vodafone Business Marketplace (“VBM”)	means the platform set out at https://marketplace.vodafone.co.uk/home .



Secure Access Gateway Service

Vodafone Business Customers

Vodafone / Vodafone Business	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 Provider acting on behalf of Vodafone,...
Vodafone Business Secure Access Gateway	means a fully provisioned, and managed cloud security control (SaaS) with Applicable Vendor technology, operated in a secure manner to protect Customer's Environment from malicious activity in accordance with Customer's security requirements.
Vodafone Group	means Vodafone Group plc and each body corporate, partnership, or unincorporated association, in respect of which Vodafone Group plc owns (directly or indirectly) at least 15 per cent of: (a) the issued share capital; or (b) the ownership interests or units issued by such partnership or unincorporated association
Zscaler	is a <u>cloud security</u> company, headquartered in <u>San Jose, California</u> . The company's cloud-native technology platform, the Zscaler zero trust exchange, is designed to help enterprise Customers secure their employees, applications, and data as infrastructure and applications move to the cloud and as employees connect to work <u>remotely</u> , off the traditional corporate <u>network</u> . See https://www.Zscaler.com/ for more details.