BT Managed Cloud Security (Zscaler) Service Schedule

BT Contract Reference:
Customer Contract Reference (optional):

1 Definitions and Abbreviations

The following definitions and abbreviations apply, in addition to those in the General Terms and Conditions.

"**Administrator**" means person authorised by the Customer who is responsible for managing the BT Managed Cloud Security (Zscaler) Service using the Customer Portal.

"**Availability Service Credit**" has the meaning given in Paragraph 18.

"**Availability Service Level**" has the meaning given in Paragraph 18.

"**Bandwidth**" means the volume of various classes of information that flows through the Customer's Internet traffic and as defined by the Customer in the Order.

"**Charges**" means those Charges set out in the Order.

"**BT Managed Cloud Security (Zscaler) Service**" means the service as set out in this Schedule.

"BT Managed Security Services" means the Graded Service Tiers provided by BT as service wrap as set out in this Schedule.

"**BT Portal**" means one or more webpages made available to the Customer by BT to allow the management of the ordered BT Managed Cloud Security (Zscaler) Services.

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

"**Co-operative Mitigation**" has the meaning as set out in Paragraph 2.3.4.

"**Complex Change**" means a change that is not a Simple Change. Examples of Complex Changes are set out in Appendix 2.

"**Continuous Improvement**" means the continuous improvement phase of the as set out in Paragraph 5.2.

"**Controlled Deployment**" means the controlled deployment phase of the ordered Graded Service Tier and the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 4.2.

"**Controlled Deployment CSP Optimisation**" means the fine tuning of the Customer's CSP(s), conducted by the Customer or in respect of Foundation Plus or Premium only both Parties jointly.

"**Controlled Deployment CSP Optimisation Period**" means in respect of:

(a) Foundation, 48 hours after receiving Notice from BT;
(b) Foundation Plus, up to 30 Business Days after receiving Notice from BT; and
(c) Premium, up to 30 Business Days after receiving Notice from BT.

"**CSP Change Management Process**" means the process in relation to changes to the CSP(s) as set out in Paragraph 5.3.

"Customer's Bandwidth Baseline" means the average per-seat bandwidth consumption calculated by the Supplier over the 90-day period following the start of Customer's subscription to the BT Managed Cloud Security (Zscaler) Service.

"**Customer Committed Date**" means the date on which BT agrees to deliver the BT Managed Cloud Security (Zscaler) Service (or each part of thereof).

"**Customer Contact**" has the meaning given in Paragraph 12.1.

"**Customer Data**" means the data inputted by the Customer or Users for the purpose of using the BT Managed Cloud Security (Zscaler) Services.

"**Customer Equipment**" means any equipment including any software, other than BT Equipment, used by the Customer in connection with a BT Managed Cloud Security (Zscaler) Service.

"**Customer Handbook**" means a document provided to the Customer upon completion of the Initial Setup phase providing Customer specific information relevant to the BT Managed Cloud Security (Zscaler) Service and Graded Service Tier purchased. The Customer Handbook is not a contractual document.

"**Customer Portal**" has the meaning given in Paragraph 2.2.2.

"**Customer Security Policy**" or "**CSP**" means the Customer's security policy containing the security rules, set and owned by the Customer, that are applied to the applicable Associated Service and determine the operation of the applicable Associated Service.

"**Customer Transaction Logs**" means, the metadata of all network traffic sent to or received by the Supplier from or to the Customer in the Customer's use of the BT Managed Cloud Security (Zscaler) Service.

"**Data Packet**" means a unit of data made into a single Internet Protocol (IP) package that travels along a given network path.

"**Devices**" means any equipment, including but not limited to laptops and servers, used by the Customer or Customer's employees to provide or gain an access to Customer's applications, systems and platforms.

"**Domain Name Service**" or "**DNS**" means a directory system which translates numeric IP addresses into Domain Names to identify users on the Internet.

"**DNS Transaction**" means a recursive DNS query sent form the Customer through its use of the BT Managed Cloud Security (Zscaler) Service.

"**Eagle-i Platform**" means the solution through which BT shall provide enriched incident alerts and identify any IOCs as part of the Eagle-i Service.

"**Eagle-i Service"** means the Service component outlined at Paragraph 2.3.3.

"**Emergency Change**" means a highly critical, Simple Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to business operations, or to prevent or resolve a P1 Incident.
"**End-User Identities**" means usernames and passwords that are used by Customer's employees to gain access to Customer's applications, systems and platforms.
"**File Transfer Protocol**" or "**FTP**" means standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.
"**Foundation**" means the Foundation Graded Service Tier as set out in this Schedule.
"**Foundation Plus**" means the Foundation Plus Graded Service Tier as set out in this Schedule.
"**Graded Service Tier**" means the term used to describe the level of management features as set out in this Service Schedule and is classified as either Foundation, Foundation Plus or Premium.
"**Hyper-Text Transfer Protocol**" or "**HTTP**" means an application protocol for distributed, collaborative, hypermedia information systems.
"**Hyper-Text Transfer Protocol Secure**" or "**HTTPS**" means a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.
"**Incident**" means an unplanned interruption to, or a reduction in the quality of the BT Managed Cloud Security (Zscaler) Service or particular element of it.
"**Indicators of Compromise**" or "**IOCs**" are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.
"**Initial Setup**" means the facilitation of the setup and delivery of the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 4.1.
"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the BT Managed Cloud Security (Zscaler) Service as applicable.
"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.
"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**In the Wild**" means a virus which is already loose in the Internet by a minimum of three (3) Wild List participants.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**Known Virus**" means a virus that, at the time of receipt of content by the Supplier: (i) a signature has already been made publicly available, for a minimum of one hour for configuration by the Supplier's third party commercial scanner; and (ii) is included on the Wild List held at http://www.wildlist.org and identified as being In the Wild.
"**Latency Service Credit**" has the meaning given to it in Paragraph 18.
"**Latency Service Level**" has the meaning given to it in Paragraph 18.
"**Location**" means a right for specific access point to the Internet in connection with the BT Managed Cloud Security (Zscaler) Service.
"**Mitigation Action**" means a recommended mitigating action which should be taken to address the impact of IOCs identified by BT.
"**Monitoring and Management**" means the monitoring and management phase of the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 5.1.
"**NSS Service**" has the meaning given to it in Paragraph 2.3.3.
"**NSS Virtual Machine**" means a machine which receives copies of traffic logs in real time via a secure tunnel in a highly compressed format from the Zscaler cloud, decompresses and detokenizes these logs, then applies specified filters and formats for streaming to a security incident and event management solution.
"**On Time Delivery Service Level**" has the meaning given in Paragraph 18.
"**Operational Service Date**" means the date on which any BT Managed Cloud Security (Zscaler) Service or part of it is first made available to the Customer by BT or the date when the Customer first starts to use such BT Managed Cloud Security (Zscaler) Service (or part of), whichever date is earlier.
"**P1**", "**P2**", "**P3**" and "**P4**" have the meaning given in the table at Paragraph 5.4.1.
"**Professional Services**" means those services proved by BT which are labour related services.
"**Prohibited Jurisdiction**" has the meaning given in Paragraph 12.3.
"**Raw Transaction Log**" means the metadata of all network traffic sent to or received from the Customer through its use of the BT Managed Cloud Security (Zscaler) Service.
"**Reasonable Use Policy**" has the meaning given in Paragraph 5.3.6.
"**Recurring Charges**" means the Charges for the BT Managed Cloud Security (Zscaler) Service (or applicable part of) that are invoiced repeatedly in every payment period (e.g. every month), as set out in the Order.

"**Renewal Period**" means for each BT Managed Cloud Security (Zscaler) Service the initial 12 month period following the Minimum Period of Service and each subsequent 12 month period, or any period as agreed by both Parties.

"**Security Operations Centre**" or "**SOC**" means the BT team responsible for the Monitoring and Management of the BT Managed Cloud Security (Zscaler) Services provided under the Graded Service Tier ordered by the Customer.

"**Security Threat Intelligence**" or "**STI**" means the security threat intelligence service set out in Paragraph 5.1.1.

"**Service Addition Request**" has the meaning given in Paragraph 14.

"**Service Credit**" means any agreed remedy for BT Supplier's failure to meet a Service Level, and, if any, as more fully described in this Schedule or set out in an Order.

"**Service Desk**" means the helpdesk that the Customer is able to contact to submit service requests, report Incidents and ask questions about the ordered Graded Service Tier and the BT Managed Cloud Security (Zscaler) Service.

"**Service Level**" means any agreed minimum level of service to be achieved by BT and its Supplier as set out in Paragraph 18.

"**Service Management Boundary**" has the meaning given in Paragraph 6.

"**Service Options**" has the meaning given in Paragraph 2.3.

"**Service Software**" means the Supplier's cloud based "**Zscaler Internet Access**" or "**Zscaler Private Access**" platform, as applicable.

"**Service Target**" means any target that BT aims to meet as set out in this Service Schedule but for which no remedy is available.

"**Session**" means any non-HTTP or HTTP request sent to or from the Customer through its use of the BT Managed Cloud Security (Zscaler) Services.

"**Simple Change**" means the Simple Changes as set out in Appendix 2 of this Schedule.

"**Standard Change**" means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements.

"**Standard Service Components**" has the meaning given in Paragraph 2.2.

"**Summarised Transaction Logs**" means the summarised versions of the Raw Transactions Logs.

"**Supplier**" means Zscaler, Inc., a Delaware corporation, having its principal place of business at 110 Baytech Drive, Suite 100, San Jose, CA 95134-2304, USA.

"**Supplier's Acceptable Use**" has the meaning given in Paragraph 12.2.

"**Supplier's Acceptable Use Policy**" means Zscaler Acceptable Use Policy as set out in Appendix 1 of this Schedule.

"**Supplier IP Rights**" has the meaning given in Paragraph 7.

"**Supplier Technology**" has the meaning given in Paragraph 7.1.

"**Surcharge Data Centres**" means the Supplier infrastructure that may be used to perform the BT Managed Cloud Security (Zscaler) Service located territories as defined by the Supplier and updated from time to time, details of which are available on request from BT.

"**Target Implementation Time**" means the target implementation time from acceptance by BT of the Customer's CSP change request as set out in the table in Paragraph 5.3.11.

"**Target Restoration Time**" has the meaning given in the table at Paragraph 5.4 for the relevant priority level and Graded Service Tier.

"**Ticket**" means the unique reference number provided by BT for an Incident that may also be known as a "**fault reference number**".

"**Transaction**" means an HTTP or HTTPS request sent to or from the Customer through its use of the BT Managed Cloud Security (Zscaler) Service.

"**Uniform Resource Locator**" or "**URL**" means a character string that points to a resource on an intranet or the Internet.

"**Urgent Change**" means in respect of a Simple Change upgrades and modifications needed as a result of unplanned activities or unforeseen activities, but which are not critical to maintaining the security of the organisation.

"**User Guides**" means the documents that set out details on how the Customer:

(a) may access the BT Portal;
(b) make changes to the CSP(s); and
(c) may access reports.

"**User Subscription**" means a right for a specific individual User to access the Internet using the BT Managed Cloud Security (Zscaler) Service. (Note: in an environment where no User authentication is present, every 2,000 DNS Transactions per day flowing through the BT Managed Cloud Security (Zscaler) Service will be attributed to one User Subscription (i.e. the number of User Subscription used would be calculated by dividing the total number of DNS Transactions flowing through the BT Managed Cloud Security (Zscaler) Service per day by 2,000).

"**Virus Capture Rate Service Credit**" has the meaning given in Paragraph 18.

"**Virus Capture Rate Service Level**" has the meaning given in Paragraph 18.

"**Wild List**" means the list of viruses "In the Wild" as maintained by the Wild List Organisation.

"**Zscaler Client Connector**" means the application allowing access to the BT Managed Cloud Security (Zscaler) Service through certain mobile operating systems and computers.

"**Zscaler Internet Access**" or "**ZIA**" means a software-based cloud service that allows a Customer to select various security options to be applied at cloud data centers across the world to protect the Customer's internet traffic.

"**Zscaler Private Access**" or "**ZPA**" means a software-based cloud service that provides seamless and secure remote access to internal applications for the Customer, regardless of where they exist, and without placing users on the Customer's network.

"**Zscaler Private Access Service Level**" has the meaning given in Paragraph 18.

"**Zscaler Private Access Service Credit**" has the meaning given in Paragraph 18.

2 Service Description

2.1 BT Managed Cloud Security (Zscaler) Service consists of:

- all the Standard Service Components set out in Paragraph 2.2; and
- any Service Options set out in Paragraph 2.3 that the Customer selects on any applicable Order.

2.2 **Standard Service Components.**

BT will provide the Customer, with all the following Standard Service Components in accordance with the details set out in any applicable Order which will comprise:

2.2.1 **Service Software**. BT will provide the Customer with the right to access and use the Service Software for the number of purchased Users, User Subscriptions and/or Locations.

2.2.2 **Portals**. BT will provide the Customer access to (a) BT Portal and (b) to the Supplier's web-based User interface ("**Customer Portal**").

(a) The BT Portal is an administrative portal of BT for accessing and managing the BT Managed Security Services.

(b) The Customer Portal is an administrative portal of the Supplier for creating and managing security policies, reporting and analysing traffic and gives the Customer a primary Administrator account that will allow the Customer to create multiple Administrators and enables the Customer to:

(i) review statistics of all malware that is stopped and other Internet content that is blocked;
(ii) create access restrictions and apply these to specific Users or groups of Users;
(iii) customise browser alert pages seen by Users when web-access is denied;
(iv) update administration details for real-time email alerts; and
(v) configure and schedule automated system auditing and reporting.

(c) The Customer may allow multiple Administrators to access the portals. The Customer shall give each of the Customer Administrator a unique login and provide management access or read only privileges specific to each Graded Service Tier. This functionality allows a unique, single super User account that can create multiple Administrators.

(d) BT may use its access rights as an Administrator to the Customer Portal to investigate and resolve any Incidents notified by the Customer to BT in accordance with Paragraph 13.

(e) BT will aim to action the Customer's request to create a new User on the BT Portal within one Business Day, except during periods of planned maintenance.

2.2.3 **BT Managed Security Services – Graded Service Tiers**. BT will provide the Customer with a range of graded security management services which can be used in association with, and as an overlay to, the BT Managed Cloud Security (Zscaler) Service; subject to following conditions:

(a) The Customer will choose one of the Graded Service Tiers, some of the features of which are set out in the table below, to use with the BT Managed Cloud Security (Zscaler) Service as set out in any applicable Order:

	Foundation	Foundation Plus	Premium
Initial Setup of the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 4.1			
Customer Security Policy			
BT Managed Cloud Security (Zscaler) Service	Good practice standard policies	Industry/scenario specific policies	Tailored security policy
BT Project Manager assigned for Initial Setup	✗ Options available as set out in Paragraph 5.1	✓ Named Options available as set out in Paragraph 5.1	✓ Named & potential Site visit depending on location.

	Foundation	Foundation Plus	Premium
On Time Delivery Service Credits for not meeting the Customer Committed Date	✗	✓	✓
Controlled Deployment of the Associated Services as set out in Paragraph 4.2			
Controlled Deployment CSP Optimisation Period commences on completion of Initial Setup			
BT Managed Cloud Security (Zscaler) Service Controlled Deployment CSP Optimisation Period	48 hrs	Up to 30 days	Up to 30 days
BT & Customer joint CSP test and tune	✗	✓	✓
Monitoring and Management of the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 5			
Security Threat Intelligence	Threat Intelligence Bulletins and Reports	As per Foundation	As per Foundation
Manage Service Incidents			
Service Desk 24x7x365	✓	✓	✓
Security Operations Centre (SOC)	BT selects appropriate SOC	BT selects appropriate SOC	BT selects appropriate SOC
Service Desk language	As agreed with BT (English by default)	As agreed with BT (English by default)	As agreed with BT (English by default)
Continuous Improvement of the BT Managed Cloud Security (Zscaler) Service as set out in Paragraph 5			
BT Graded Service Tiers and BT Managed Cloud Security (Zscaler) Service reviews	6 monthly	Quarterly	At intervals agreed by both Parties
Change Management	via the BT Portal	Via the BT Portal or the appropriate BT Personnel	via the BT Portal or the appropriate BT Personnel

(b) The Graded Service Tier selected with the initial Order shall also apply for any future Orders the Customer may place for BT Managed Cloud Security (Zscaler) Services as the Customer cannot have more than one Graded Service Tier.

(c) During the Minimum Period of Service or any subsequent renewal period the Customer may upgrade to a higher Graded Service Tier, but the Customer may not downgrade to a lower Graded Service Tier. Any new Charges and a new Minimum Period of Service for the upgraded Graded Service Tier will be agreed by a new Order. No Termination Charges will be payable from the Graded Service Tier the Customer is moving from.

(d) If there is a conflict between the provisions of the Graded Service Tiers, the order of priority of the relevant provision, depending on the Graded Service Tier ordered by the Customer, is the following:

(i) Premium;
(ii) Foundation Plus;
(iii) Foundation.

2.3 Service Options

The Customer may order any of the following options as further specified (including any additional Charges) in any applicable Order:

2.3.1 **Surcharge Data Centres**: In certain countries or regions BT or the Supplier may suggest that the Customer data be hosted and processed in Surcharge Data Centres. Where the Customer selects this option, it will incur additional Charges, which will be set out in the Order. The Customer may choose to use Supplier data centres other than the Surcharge Data Centres, but it acknowledges that performance of the Service may be affected; and

2.3.2 **Professional Services**: BT may provide, at an additional Charge, Professional Services with each Order, to support the Customer`s initial configuration of the Service and the ongoing operation of the Service.

2.3.3 **Eagle-i-Service:** For Foundation Plus and Premium Graded Service Tiers, BT will include a subscription to the Eagle-i Service with each Order subject to the following.

(a) The Eagle-i Service ingests Zscaler Nanolog Streaming Service ("NSS Service") logs from the Managed Cloud Security Service, whereby BT will:

(i) monitor the NSS Service logs for events and enrich with BT's threat intelligence;
(ii) alert the Customer of high priority security incidents; and
(iii) BT will, where applicable, recommend a proposed Mitigation Action.

(b) If the Customer already has an existing NSS Service, the Customer shall provide BT with a data feed from the Customer's existing NSS Service.

(c) If the Customer does not have an existing NSS Service, the Customer must select one of the following at the outset of an Order;

(i) hosting of the NSS Virtual Machine by BT; or
(ii) hosting of the NSS Virtual Machine by the Customer. In such case, the Customer will, when placing the Order with BT, inform BT that the NSS Virtual Machine will be hosted by the Customer and provide BT with a data feed from the NSS Service to the Service.

(d) If the Customer selected the Foundation Plus Graded Service Tier on the Order; the Customer shall be responsible for implementing any Mitigation Action, which shall be actioned by accessing the relevant service management tool for the impacted components.

(e) If the Customer selected the Premium Graded Service Tier on the Order, the Customer may select **Co-operative Mitigation** on the Order. Subject to paragraph 12.1.12, BT will in the event of a detected Incident apply Mitigation Action on specific endpoint Devices or End-User Identities identified to BT where:

(i) the impact of the detected Incident will be contained; and
(ii) appropriate changes are made by BT to the security policy or other Eagle-i services on the Premium Graded Service Tier.

2.3.4 **Co-Management**: BT will provide the Customer with a RBAC Profile("**Role Based Account Control Profile**") for up to a maximum of 5 authorised nominated Users on the Customer Portal. Users utilizing the RBAC Profile will have restricted access to implement Simple Changes. If the Customer orders Co-Management:

(a) the Customer will be responsible for ensuring that the authorised nominated Users complete the Customer Portal training available from the Supplier, at Customer's own cost before these Users are allowed to implement Simple Changes;

(b) BT will provide a separate user guide to the Customer setting out details how to manage Simple Changes;

(c) In variance to what is set out in Paragraph 5.3, the Customer will be responsible for implementing the Simple Changes including the impact of such changes and BT will not be liable for any consequences arising from this action, including but not limited to performance issues or outages to the Service; and

(d) if a Simple Change implemented by any User using the RBAC Profile has resulted in an Incident,

(i) the Customer will notify the Incident in accordance with Paragraph 13;
(ii) BT will provide assistance to resolve the Incident in accordance with Paragraph 5.4 using the audit and logging capability on the Customer Portal to support any root cause analysis undertaken to confirm this; and
BT reserves the right to implement applicable Charges for any corrective action that would be required to rectify.

3 Minimum Period of Service and Renewal Periods

3.1 Unless otherwise agreed on an Order, the Minimum Period of Service will be a period of twelve (12) consecutive months beginning on the Operational Service Date. The Service ends automatically at the end of the Minimum Period unless the Parties agree to renew the Service with a Renewal Period at least 90 days before the end of the Minimum Period of Service or each Renewal Period by signature of a new Order.

3.2 In the event that both Parties wish to continue to supply and use the BT Managed Cloud Security (Zscaler) Service, BT may propose changes to this Schedule, the Charges and/or the General Terms and Conditions by giving the Customer at least 60 days prior written notice before the end of the Minimum Period of Service and each Renewal Period.

3.3 Any such changes should be agreed in writing between the Parties within 30 days after receipt of BT's notice to amendment.

3.4 In the event the changes are agreed between the Parties these will apply from the beginning of the following Renewal Period and the contract extended, during which time:

(a) BT will continue to provide the BT Managed Cloud Security (Zscaler) Service; and

(b) each Party will continue to perform its obligations in accordance with the Agreement.

3.5 In the event the Parties cannot agree on the required changes; then the BT Managed Cloud Security (Zscaler) Service shall end and BT will cease delivering the BT Managed Security Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

4 Service Delivery

4.1 **Initial Setup**

BT will agree with the Customer a date for implementation of the Service. Following delivery options will apply depending on the respective Graded Service Tier selected by the Customer:

4.1.1 **Foundation**

- **Standard included with Foundation.**

(a) BT responsibilities:

(i) BT will keep the Customer informed throughout the delivery process.

(ii) BT will provide standard polices that reflect good practice.

(iii) BT will co-ordinate the delivery of the BT Managed Cloud Security (Zscaler) Services.

(iv) BT will commission the BT Managed Cloud Security (Zscaler) Services remotely in accordance with the CSP(s) policies selected by the Customer, unless set out otherwise in this Service Schedule.

(v) on the date that BT has completed its delivery activities as set out in the BT Managed Cloud Security (Zscaler) Service Schedule and this Service Schedule, BT will confirm to the Customer the date that the Initial Setup is complete. This will be the Operational Service Date and from that date the Controlled Deployment CSP Optimisation Period will commence.

(b) Customer responsibilities:

(i) The Customer will select appropriate policies to use as the Customer's CSP(s) when the Customer places the Order and ensures that the standard policies the Customer selects meet the Customer's requirements. The Customer remains responsible for defining the Customer's ongoing CSP(s) beyond that set out in the policies selected by the Customer after the Operational Service Date.

(ii) The Customer may request changes to the Customer's CSPs after the Operational Service Date in accordance with Paragraph 14.

- **Optional with Foundation.**

The Customer may request that BT, at an additional Charge to be agreed by the Parties and set out in the Order:

(a) appoints a named BT Project Manager to be the Customer's single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit the Customer's Site;

(b) provides a named BT Project Manager who will be available to attend meetings at the Customer's Site depending on the Customer's location for the duration of the Initial Setup; or

(c) provides the Customer with Professional Services to assist the Customer in the creation of the Customer's CSP(s). The responsibility for the CSP(s) will remain with the Customer.

4.1.2 **Foundation Plus.** In variance to the provisions as set out in Paragraph 4.1.1, Foundation;

- **Standard included with Foundation Plus.**

(a) BT will appoint a named BT Project Manager to be the Customer's single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit the Customer's Site; and

(b) BT will provide a customisable security policy to use as the Customer's CSPs.

- **Optional with Foundation Plus.**

The Customer may request that BT provides a named BT Project Manager who will be available to attend meetings at the Customer's Site depending on the Customer's location for the duration of the Initial Setup at an additional Charge to be agreed by the Parties and set out in the Order.

4.1.3 **Premium.** In variance to the provisions as set out in Paragraph 4.1.1, Foundation and Paragraph 4.1.2, Foundation Plus;

(a) BT will provide a named BT Project Manager who will be available to attend meetings with the Customer at the Customer's Site depending on the Customer's location for the duration of the Initial Setup; and

(a) the Customer will appoint a Customer project manager and technical team who will work with BT during the Initial Setup; particularly during the Controlled Deployment Optimisation Period as set out in Paragraph 5 below.

4.2 **Controlled Deployment**

BT will provide activation support to the Customer so that the Customer has access to the Customer Portal for configuration of the Service. BT will deploy the Service using one or more of the supply methods set out at: https://zscaler.zendesk.com/hc/en-us/articles/205118615 - Choosing-Traffic-Forwarding-Methods (or any other online address that BT may advise the Customer of) and, if the Customer has chosen to include the deployment services option in the Services, BT will work with the Customer to decide which method of deployment to use. BT will work with the Customer to prepare a deployment plan during the Controlled Deployment CSP Optimisation Period in accordance with following provisions depending on the respective Graded Service Tier selected by the Customer:

4.2.1 **Foundation**

(a) BT will provide the Customer with User Guides.
(b) The Customer will comply with the User Guides.
(c) The Customer will carry out the Controlled Deployment CSP Optimisation within the Controlled Deployment CSP Optimisation Period.
(d) The Customer will notify BT when the Customer has completed the Controlled Deployment CSP Optimisation. If the Customer does not provide BT with such notice by the end of the Controlled Deployment CSP Optimisation Period, the Controlled Deployment CSP Optimisation will be deemed to have been completed by the Customer.
(e) BT will notify the Customer of the date of completion of the Controlled Deployment CSP Optimisation.
(f) The Customer will submit any changes the Customer requires to the CSP as a result of the Controlled Deployment CSP Optimisation through the CSP Change Management Process as set out in Paragraph 5.3.
(g) If the Customer has requested changes to the CSP(s) during the Controlled Deployment CSP Optimisation Period, BT will direct the Customer to the CSP change management facility on the Security Portal if the Customer's request for the change to the CSP(s) is outside the BT Managed Security Service and the BT Managed Cloud Security (Zscaler) Services. The Customer will follow the CSP Change Management Process set out in Paragraph 5.3. If BT is aware that, or the Customer advises BT that, the Customer is unable to access the BT Portal, BT will direct the Customer to the appropriate BT personnel to review the Customer's request.

4.2.2 **Foundation Plus and Premium.** In variance to the provisions as set out in Paragraph 4.2.1, Foundation;

Both Parties will jointly carry out the Controlled Deployment CSP Optimisation. The Customer will use reasonable endeavours to complete the Controlled Deployment CSP Optimisation as early into the Controlled Deployment CSP Optimisation Period as possible.

4.3 **Notification of Service provision**

BT will notify the Customer that the Service has been enabled, and provide activation support to the Customer. The Operational Service Date occurs once BT notifies the Customer that the Service has been enabled. BT will send a provisioning email to the Customer that will provide Customer Portal log in information and a Customer welcome letter.

5 In Life Management

5.1 **Monitoring and Management**

The following Monitoring and Management services will be provided by BT, commencing from the Operational Service Date:

5.1.1 **Security Threat Intelligence.** With each Graded Service Tier; BT will provide the Customer with the following general intelligence bulletins and reports in English to an agreed list of Customer Contacts:

(a) daily threat advisories: these provide a view of the latest headline security events, actors, targets, operations and campaigns, vulnerabilities and suspicious IP Addresses;
(b) global threat summaries: these provide a wide angle and high-level view of the significant events and attacks that have occurred globally and across all industries;
(c) monthly executive level briefing: these provide a CISO level view of the threat landscape focussing on events impacting global organisations from a strategic perspective; and
(d) global critical bulletins: these provide a technical assessment of significant global security events such as WannaCry so that a more detailed understanding can be obtained.

5.1.2 **Manage Service Incidents**

BT will act as a single point of contact for resolution of Incidents related to the BT Managed Cloud Security (Zscaler) Services; depending on the respective Graded Service Tier selected by the Customer:

5.1.2.1 **Foundation**

(a) The Customer will only notify Incidents via the BT Portal.

(b) All communications with the Service Desk will be in English.

(c) The Service Desk that will action the Incident notifications is available 24x7x365 and is staffed by security trained professionals.

(d) BT will give the Customer a Ticket.

(e) BT will assess the Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	One or more core Sites or Services are completely unavailable, or one or more core functions of the Associated Services are completely unable to be performed. For User-based services (e.g. MS Teams), this would typically be all Users.
P2	Material impact to Associated Service e.g., a partially interrupted or impaired Service which cannot be mitigated, or core business functions can be performed but in a reduced capacity. This priority level would also apply for the loss of a non-core site or Service.
P3	Medium impact to Associated Service, e.g., a Site or Service experiencing intermittent or localised interruption or impairment. This might be an issue where a large percentage of the Associated Service is functioning normally, such as the Site is suffering slow response, but Users are able to work, a small number of Users at a Site have total loss of service but the majority are functioning normally, or perhaps one element of Service is unavailable, such as access to voicemail. A P3 incident would also be raised for a resilient Site where either the primary or resilient path is unavailable.
P4	Typically very minor or no impact on Associated Services, such as a single User or very small number of Users having minor issues but core functions of the Associated Services can be carried out as normal.

(f) BT will review the status of the Incident and amend the priority level assigned initially if necessary.

(g) BT will keep the Customer informed throughout the course of the Incident resolution at regular intervals by posting updates on the BT Portal or via e-mails to the Customer Contact.

5.1.2.2 **Foundation Plus.** In variance to the provisions as set out in Paragraph 5.1.2.1, Foundation;

the Customer may also notify all Incidents directly to the Service Desk.

5.1.2.3 **Premium .** In variance to the provisions as set out in Paragraph 5.1.2.1, Foundation and Paragraph 5.1.2.2 Foundation Plus;

the Customer may also notify all Incidents directly to the regional Security Operations Centre.

5.2 Continuous Improvement

The following additional Continuous Improvement services will be provided by BT, commencing from the Operational Service Date:

5.2.1 **Reviews**

5.2.1.1 **Foundation**

(a) The Security Optimisation Manager will carry out a review six (6) monthly as follows:

(i) a service review focussing on the performance of the BT Graded Service Tier and the BT Managed Cloud Security (Zscaler) Service; and

(ii) an end of life review on an ongoing basis. The Security Optimisation Manager will provide the Customer with a report summarising the applications and software that are managed by BT on the Customer's behalf as part of the BT Managed Cloud Security (Zscaler) Services that will go end of life within the following six months. The report will include applications and software advised to the Customer previously that are past end of life and that require immediate action by the Customer.

(b) If requested by the Customer and if agreed to by BT, both Parties may hold a conference call to discuss the report.

(c) If BT has agreed to participate in a conference call the Customer will ensure that any report the Security Optimisation Manager provides the Customer with will be reviewed by the Customer's suitably qualified personnel who are participating in the conference call prior to the conference call taking place.

(d) The Customer will take appropriate action to address issues as recommended by the Security Optimisation Manager:

(i) in respect of the BT Graded Service Tier and the BT Managed Cloud Security (Zscaler) Service including implementing security improvements as agreed with the Security Optimisation

Manager or as advised by the Security Optimisation Manager as the Customer's responsibility; and

(ii) in respect of the end of life review or as set out in the end of life review report.

5.2.1.2 **Foundation Plus.** In variance to the provisions as set out in Paragraph 5.2.1.1, Foundation;

(a) The Security Optimisation Manager will carry out a review quarterly as follows:

(i) a service review focussing on the performance of the BT Graded Service Tier and the BT Managed Cloud Security (Zscaler) Service against Service Levels and Service Targets and capacity management of the BT Managed Cloud Security (Zscaler) Service;

(ii) a review of the Customer's CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of the Customer's CSP(s); and

(b) In addition to taking the action set out in Paragraph 5.2.1.1(d), the Customer will be responsible for initiating the appropriate change requests in accordance with the CSP Change Management Process to address issues in respect of fine tuning or amending the Customer's CSP(s) as recommended by the Security Optimisation Manager.

5.2.1.3 **Premium.** In variance to the provisions as set out in Paragraph 5.2.1.1, Foundation and Paragraph 5.2.1.2, Foundation Plus;

(a) The Security Optimisation Manager will carry out the reviews as set out in Paragraph 5.2.1.2 (a) at intervals agreed by both Parties but not less than monthly.

(b) The Security Optimisation Manager will provide the Customer with a report on the review via the BT Portal or direct to the Customer by e-mail, if agreed by both Parties.

(c) If requested by the Customer and if agreed to by BT, both Parties may hold a conference call to discuss the report or BT may attend a meeting at the Customer's Site depending on the Customer's location to discuss the report with the Customer. In such event the Customer will ensure that any report the Security Optimisation Manager provides the Customer with will be reviewed by the Customer's suitably qualified personnel who are participating in the conference call or attending the meeting prior to the conference call taking place

5.3 CSP Change Management Process

5.3.1 BT will implement changes to the CSP(s) in response to Customer's request subject to the following process ("CSP Change Management Process") and depending on the Graded Service Tier as set out on the Order:

BT Support	Foundation	Foundation Plus	Premium
Customer requests to be initiated.	through the BT Portal	through the BT Portal or direct to the Security Optimisation Manager	through the BT Portal or direct to the Security Optimisation Manager
Identification by BT of errors or potential unforeseen consequences of Customers requested Simple Changes and Complex Changes	✗	✗	✓
Simple Changes - Standard changes (*)	ZIA 6 per month	ZIA 8 per month ZPA 8 per month	ZIA 10 per month ZPA 10 per month
Simple Changes - Urgent changes	1 per month	2 per month	3 per month
Simple Changes - Emergency Changes	Charged at the rate of a Simple change.	Charged at the rate of a Simple change.	Charged at the rate of a Simple change.
Complex changes	To be agreed by a new Order	To be agreed by a new Order	To be agreed by a new Order

Note: Reasonable Use Policy restrictions for Standard Change requests set out in Paragraph 5.3.6 of this Schedule will apply each to Zscaler Internet Access and Zscaler Private Access.

5.3.2 The authorised Customer Contact will submit requests to change the CSP(s) and will provide sufficient detail and clear instructions as to any changes required. The Customer will not, and ensure that Users with access to the BT Portal do not, submit any unauthorised changes. If BT is aware that, or the Customer advises that, the Customer is unable to access the BT Portal, BT will direct the Customer to the appropriate BT personnel to review the Customer request.

5.3.3 BT will check each request for its complexity and assess whether the change (i) should be completed via the CSP Change Management Process, (ii) requires a new Order or (iii) requires a contract change to be agreed by a written amendment to the Agreement.

5.3.4 Only CSP changes to rule-sets that define the operation of the Service will be completed via the CSP Change Management Process.

5.3.5 For the avoidance of doubt; any change whereby the Customer requests changes to the Service not being qualified as Simple Change (e.g. including additional licences) requires a new Order.

5.3.6 Standard and Urgent Changes are included in the Charges subject to the limitations as set out in above table ("**Reasonable Use Policy**"). Where Standard and/or Urgent Changes are being raised more frequently; the Parties may either agree:

(a) to aggregate the Customer requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays;

(b) to review the Customer requirements and agree with the Customer an appropriate alternative implementation process and any associated charges via a new Order; or

(c) to charge such additional change request at the rate as set out in the Order.

5.3.7 Complex Change requests will be agreed between the Customer and BT via a new Order; including any additional Charges for implementing such Complex Changes.

5.3.8 Any Emergency Change will be implemented by BT as quickly as is reasonably practicable and without Customer's prior approval; subject that BT afterwards demonstrate why such Emergency change was required.

5.3.9 BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change and the status will be available also on the BT Portal for a period of six months.

5.3.10 Except for Emergency Changes,

(a) the Customer is deemed to have approved all changes to the CSP(s) that are submitted to BT; and

(b) the Customer is responsible for the impact of BT implementing the changes. This means if BT implements this change in accordance with the Customer request, BT will not be liable for any consequences arising from the impact of the implementation of the changes; including any misspecification of the Customer security requirements in the CSP(s) or any unforeseen consequences of a correctly specified and correctly implemented CSP(s).

5.3.11 In the event the Customer has ordered Foundation Plus or Premium; BT will aim to implement changes to the Customer's CSP(s) in accordance with the table set out below:

Request	Target Implementation Time
Simple Change - Standard Change	8 Hours calculated from the moment BT accepted the Customer's change request.
Simple Change - Urgent Change	4 Hours calculated from the moment BT accepted the Customer's change request.
Simple Change - Emergency Change	4 Hours calculated from the moment identified the need for an Emergency Change.
Complex Change	As agreed on the Order

5.3.12 The Customer may order Professional Services to assist the Customer in writing the change request.

5.4 Response Times – Service Targets for Incident Management

5.4.1 BT will respond to Incidents, depending on the respective Graded Service Tier selected by the Customer, in line with the following table and this starting from when the Service Desk provides the Customer with a Ticket:

	Incident Stage			
Priority	**Initial Response**	**Next Response**	**Further Responses**	**Target Restoration**
P1	the Customer will be informed that BT is dealing with the Incident within 15 minutes of receiving it (either via an alert or by the Customer advising BT)	First update within 30 minutes from the Incident ticket being opened	Every 60 minutes	4 hours

P2	the Customer will be informed that BT is dealing with the Incident within 30 minutes of receiving it (either via an alert or by the Customer advising BT)	First update within 60 minutes from the Incident ticket being opened	Every 2 hours	8 hours
P3	N/A	First update within 4 hours from the Incident ticket being opened	Every 4 hours	24 hours
P4	N/A	First update within 24 hours from the Incident ticket being opened	Every 24 hours	48 hours

5.4.2 BT will aim to provide the Customer with an update on the progress of an Incident in accordance with the table above.

5.4.3 BT will not provide a progress update while BT is waiting on the Customer's input or feedback. The total time when the ticket is in pending status will be excluded when measuring both response and restoration timings and when measuring availability of the Service.

5.4.4 BT will aim to restore the BT Managed Cloud Security (Zscaler) Service affected by the Incident within the period set out in the table above.

5.4.5 The progress update times and restoration times are targets only and BT will have no liability for failure to meet them.

5.4.6 The Customer will allow BT to run discovery tools on the Customer's network to enhance and fine tune the Customer's CSP(s) or to assist in the resolution of Incidents.

6 Service Management Boundary (SMB)

6.1 BT will provide and manage the Service as set out in this Schedule and as set out in the Order. The Service management boundary is the point where traffic enters and leaves the infrastructure owned or controlled by the Supplier.

6.2 BT will have no responsibility for the Service outside the Service Management Boundary, including but not limited to:

6.2.1 issues on User machines (e.g. operating system, coding languages and security settings);

6.2.2 end to end network connectivity (e.g. the Customer's network or networking equipment, Internet connectivity);

6.2.3 identity source management;

6.2.4 policy ownership; or

6.2.5 security information and event management analysis.

6.2.6 Where BT is required to link to or utilise a non-BT provided network to enable BT to provide the Graded Service Tier to the Customer, and there is a subsequent failure to the third party network which causes disruption to BT's ability to provide the Graded Service Tier,

(a) BT will have no liability to the Customer relating to provision and performance of the Graded Service Tier and BT's inability to provide the Graded Service Tier, or its effect on other associated services;

(b) the Service Levels and Service Targets will not apply; and

(c) if BT is required to carry out additional work to resolve any issues arising, the Parties will agree the additional work and additional Charges for such work in writing in an Order.

6.3 BT does not guarantee that the Service will detect or block all malicious threats. The Customer acknowledges that the Service cannot ensure prevention or detection of all threats and unauthorised actions.

6.4 BT does not make any representations, whether express or implied, about the interoperability between the Service and any Customer Equipment.

6.5 While the Eagle-i Service (if selected as part of the Order) aims to significantly reduce the impact of threats on the endpoint Device or End-User Identities identified to BT, BT does not make any representations or warranties, whether express or implied that all threats will be mitigated.

6.6 When Co-operative Mitigation with Premium Graded Services is selected by the Customer, BT's responsibility is limited to providing Co-operative Mitigation on endpoint Devices or End-User Identities other than those identified to be excluded by BT and BT is not responsible for any impact on other excluded endpoint Devices or any other Equipment owned by the Customer or Customer wider network. If the Customer has selected that the Customer wishes to approve each Mitigation Action, BT will only apply this Mitigation Action once the Customer has given such approval.

6.7 Certain Service Options may require the Customer having specific Customer Equipment that meets minimum specifications, communicated to the Customer by BT or the Supplier, to benefit from full functionality. BT will not be responsible for any inability to provide the Service or degradation of the Service where the Customer uses the Service without the required Customer Equipment.

7 Supplier Intellectual Property

7.1 The Supplier uses:

7.1.1 product names associated with the Service and other trademarks;

7.1.2 certain audio and visual information, documents, software and other works of authorship; and

7.1.3 other technology, software, hardware, products, processes, algorithms, user interfaces, know-how and other trade secrets, techniques, designs, inventions and other tangible or intangible technical material or information,

(together, the "**Supplier Technology**").

7.2 The Supplier Technology is protected by intellectual property rights owned or licensed by the Supplier ("**Supplier IP Rights**").

7.3 All rights, title and interest in and to the Software and the Service Software, and all associated Supplier IP Rights, will at all times remain vested in the Supplier and its licensors, and, other than the rights granted in this Service Schedule, the Customer will acquire no other rights, express or implied, in the Service.

8 Customer Transaction Logs

8.1 BT and the Supplier may use, reproduce, store, modify, and display the information from the Customer Transaction Logs for the purpose of providing the Service.

8.2 BT and the Supplier may, use the malware, spam, botnets or other information related to the Service for the purpose of:

(a) maintaining and improving the Service;
(b) complying with all legal or contractual requirements;
(c) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service;
(d) anonymously aggregating and statistically analysing the content; and
(e) other uses related to the analysis of the Service.

8.3 In the case of Zscaler Internet Access, the Supplier will retain Raw Transaction Logs, the Summarised Transaction Logs and any other Customer Transaction Logs for rolling six month periods during the provision of the Service.

8.4 In the case of Zscaler Private Access, the Supplier will retain the Raw Transaction Logs for rolling two week periods during the provision of the Service

8.5 Upon termination of the Service, the Supplier will delete the Customer Transaction Logs, in accordance with the two-week or six-month retention cycle set out above, unless the Customer requests in writing to BT that the Customer Transaction Logs are maintained for an additional time period, which will be subject to agreement and an additional charge to be agreed between the Customer and BT by written Order.

9 Suggestions, Ideas and Feedback

The Customer agrees that the Supplier and/or BT will have the right to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by the Customer relating to the Service, to the extent it is not Customer's confidential information.

10 Excessive Bandwidth Consumption

10.1 If the 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, the Customer will be notified and the Customer agrees to work with BT and the Supplier in good faith to investigate the reason(s) for Customer's bandwidth increase (e.g. additional non-purchased seats using the BT Managed Cloud Security (Zscaler) Service, non-seat traffic using the BT Managed Cloud Security (Zscaler) Service, changes in Customer's network, etc.). The Customer and BT will either agree on a bandwidth reduction plan or the Customer will order additional capacity (additional gigabytes of monthly traffic which will be pro-rated and co-terminous with the then-current Minimum Period of Service.

10.2 If Customer does not either reduce its monthly traffic or order additional capacity (e.g. seats, servers, and/or additional gigabytes of monthly traffic) within ninety (90) days of notification, then the Customer shall be invoiced for the required additional capacity starting from the date of notification.

11 Service Software

BT and its Supplier does not warrant the Service Software to access the Customer Portal will be fault free; but BT and its Supplier shall use all reasonable endeavours to solve any issues without undue delay.

12 The Customer's Responsibilities

12.1 The Customer will be responsible for the following:

12.1.1 providing BT with the names and contact details of any Administrators authorized to act on the Customer's behalf for Service management matters ("**Customer Contact**") provision and maintenance of and payment for its access connection to the Internet or any equipment necessary to make such connection;

12.1.2 reporting any Incidents on the Internet connections directly to the BT of the compatible Internet connections;

12.1.3 directing external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executable) through the Service. The configuration settings required to direct this external traffic via the Service are made and maintained by the Customer (with assistance and support from BT as reasonably required) and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/HTTPS/FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Service;

12.1.4 supplying BT with any technical data and any other information BT may request from time to time to allow BT to supply the Service;

12.1.5 informing BT 14 days in advance and provide details of any changes to the Customer network that may impact the working of the Service. If this information is not provided, BT may be delayed or unable to arrange for any necessary changes to the Service configuration and will have no liability for such delay or failure;

12.1.6 creating their own login/password combinations ("**IDs**") for access to the Customer Portal for use by the Customer or its Users. At the Customer's sole discretion, the Customer may assign one (1) login combination to BT personnel. The Customer is responsible for its Users' use of these ID's and for downloading and installing Software if required;

12.1.7 all aspects of security policy configuration, including setting up any User groups that may be required on the Customer's authentication server which the Customer will reflect in the Customer's security policy. This is done via the Customer Portal. Where the Customer has requested BT to configure the security policy, BT will do so, prior to the Operational Service Date, and subsequently, at an additional Charge, and the Customer will be responsible for defining the Customer's security policy and for any consequences arising from a misspecification of the Customer`s security requirements, or from unforeseen consequences of a Service configuration that contains misspecifications but is correctly implemented by BT;

12.1.8 ensuring that each User Subscription purchased by the Customer will be used only by a single, individual named User and a User Subscription may never be shared between or used by more than one individual. The Customer acknowledges and agrees that a User Subscription may only be transferred from one individual to another if the original individual is no longer permitted to access, and does no longer access, the Internet in connection with the BT Managed Cloud Security (Zscaler) Services.

12.1.9 ensuring to order the appropriate BT Managed Cloud Security (Zscaler) Service features for its requirements;

12.1.10 carrying out all of its other responsibilities set out in this Schedule in a timely and efficient manner. If there are any delays in completion of the Customer responsibilities, BT may adjust any agreed timetable or delivery schedule as reasonably necessary;

12.1.11 where applicable, deployment of the Zscaler Client Connector on Users' devices and the configuration and management of all settings relevant to the Zscaler Client Connector; and

12.1.12 when the Customer orders Co-operative Mitigation option with Premium Graded Service Tiers; the Customer will:

(a) agree in the Order that BT is authorised to not take Mitigation Action in relation to specific security controls, and where appropriate specific endpoint Devices or End-User Identities;

(b) select in the Order if such is done either automatically or subject to Customer's approval; and

(c) securely provide BT with the necessary access credentials to the platforms that are used by the Customer to make policy changes to the endpoints or End-User Identities requiring Co-operative Mitigation and notify BT of any subsequent changes to these credentials.

12.2 **Supplier Acceptable Use**

12.2.1 The Customer will use the BT Managed Cloud Security (Zscaler) Service solely for the Customer's business purposes and will only permit access to the BT Managed Cloud Security (Zscaler) Service by the Customer`s employees, agents and third parties authorized by the Customer to use the BT Managed Cloud Security (Zscaler) Service.

12.2.2 The Customer will not, and will not permit or encourage Users to:

(a) modify, copy or make derivative works based on the Supplier Technology;

(b) disassemble, reverse engineer, or decompile any of the Supplier Technology;

(c) create Internet "**links**" to or from the BT Managed Cloud Security (Zscaler) Service, or "**frame**" or "**mirror**" any of the Supplier's content that forms part of the BT Managed Cloud Security (Zscaler) Service (other than on the Customer's own internal intranet); or

(d) use the BT Managed Cloud Security (Zscaler) Service for running automatic queries to websites.

12.2.3 The Customer will comply with the Supplier's Acceptable Use Policy as set out in Appendix 1.

12.2.4 BT or the Supplier, may block source IP Addresses or suspend the Customer`s access to the BT Managed Cloud Security (Zscaler) Service if the Customer`s use of the BT Managed Cloud Security (Zscaler) Service does not comply with this Service Schedule or the Agreement.

12.3 **Prohibited Jurisdictions**

12.3.1 In addition to any other compliance obligations; the Customer will not and the Customer will not allow Customer's Users to access or use the BT Managed Cloud Security (Zscaler) Service directly or indirectly in violation of any U.S. or other applicable export control or economic sanctions laws; ("**Prohibited Jurisdiction**")

12.3.2 The Customer warrants that:

(a) the Customer is not named on any US government list of persons or entities prohibited from receiving US exports or transacting with any US person; and

(b) the Customer is not a national of, or a company registered in any Prohibited Jurisdiction.

13 Notification of Incidents

Where the Customer becomes aware of an Incident:

13.1 the Customer Contact will report it to BT's Service Desk;

13.2 BT will give the Customer a **Ticket**;

13.3 BT will inform the Customer when it believes the Incident is cleared, and will close the Trouble Ticket when:

(a) the Customer confirms that the Incident is cleared within twenty-four (24) hours of being informed; or

(b) BT has attempted unsuccessfully to contact the Customer, in the way agreed between them both, in relation to the Incident and the Customer has not responded within twenty-four (24) hours of BT's attempt to contact the Customer.

13.4 If the Customer confirms that the Incident is not cleared within twenty-four (24) hours of being informed, the Ticket will remain open, and BT will continue to endeavour to resolve the Incident, until the Ticket is closed as set out in Paragraph 13.3.

13.5 Where BT becomes aware of an Incident, Paragraphs 13.1 and 13.4 will apply.

14 Changes to Customer Requirements / Service Addition Request

14.1 The Customer may submit a Service Addition Request to inform BT to:

14.1.1 make any changes in the existing BT Managed Cloud Security (Zscaler) Service;

14.1.2 increase the number of Users using the BT Managed Cloud Security (Zscaler) Service; and/or

14.1.3 select Additional Features in addition to those selected as part of the Customer's initial Order,

and where BT agrees to the change the Customer will pay any additional Charges.

14.2 If the number of Users exceeds the ordered limit as demonstrated by BT via the management reports, BT will notify the Customer and the Parties may:

14.2.1 Agree a new Order with the increased number of Users and any new Charges within 30 days; or

14.2.2 Agree that the Customer shall reduce the number of Users using the BT Managed Cloud Security (Zscaler) Service within five (5) Business Days from the date, where either party states that there is no agreement on an increased order and new Charges.

14.3 If the Parties agree to increase the number of Users and/or select Additional Features to those selected as part of the Customer's initial order:

(a) more than six months before the end of the Minimum Period of BT Managed Cloud Security (Zscaler) Service or Renewal Period, new (increased) Charges need to be agreed on the new agreed Order; or

(b) less than six (6) months before the end of the Minimum Period of BT Managed Cloud Security (Zscaler) Service or Renewal Period, this will be subject to review and acceptance by BT.

14.4 The Customer will not reduce the number of Users, User Subscriptions or BT Managed Cloud Security (Zscaler) Service components at any time after the Operational Service Date.

14.5 Where the Customer has ordered Co-operative Mitigation with Premium Graded Services, the Customer may deselect the Co-operative Mitigation option of the Service entirely or partly at any time subject to the following:

(a) the Customer shall notify BT and BT will confirm the date from which the Mitigation Action component will be de-activated from the Service;
(b) the Customer shall remove BT's access credentials to endpoint Device or End-User Identities;
(c) the Customer shall from the date of de-activation be responsible for implementing any Mitigation Action which BT recommends; and
(d) for the avoidance of doubt, deselection of the Co-operative Mitigation component of the Service shall not result in any reduction to the Charges which are payable in line with the selected Service Tier.

15 Charges and Payment Terms

15.1 The Customer will pay the Charges in accordance with the General Terms and Conditions of the Agreement.

15.2 Unless stated otherwise in an applicable Order, BT will invoice the Customer from the Operational Service Date for:

15.2.1 Any set-up Charges as detailed in the Order;

15.2.2 Recurring Charges for:

(a) the applicable Service Software licence;
(b) for any applicable Suites and Additional Features, including for the use of Surcharge Data Centres if ordered by the Customer;

Charges will be invoiced monthly in advance. Where BT Managed Cloud Security (Zscaler) Service is provided for less than the relevant invoicing period, the recurring Charges will be calculated on a monthly or daily basis as applicable.

15.2.3 Any other Charges as set out in any applicable Order; e.g. extra Charges for expediting provision of the BT Managed Cloud Security (Zscaler) Service at the Customer's request.

15.2.4 Any termination Charges in accordance with Paragraph 16 of this Schedule:

15.3 BT may invoice the Customer for any of the following Charges in addition to those set out in the Order:

15.3.1 Charges for investigating Incidents reported by the Customer, where BT finds no Incident or that the Incident is outside the Service Management Boundary;

15.3.2 Charges for commissioning the BT Managed Cloud Security (Zscaler) Service outside of Business Hours;

15.3.3 Charges for restoring BT Managed Cloud Security (Zscaler) Service if the BT Managed Cloud Security (Zscaler) Service has been suspended in accordance with the Agreement; or

15.3.4 Charges for cancelling the BT Managed Cloud Security (Zscaler) Service in accordance with the General Terms and Conditions.

16 Termination Charges

16.1 If the Customer exercises its right under the General Terms and Conditions to terminate the BT Managed Cloud Security (Zscaler) Service for convenience, the Customer shall pay:

16.1.1 all outstanding Charges for BT Managed Cloud Security (Zscaler) Services rendered.

16.1.2 all incremental charges that BT incurs from the Supplier due to the early termination, if applicable.

16.2 In addition to the Charges set out at Paragraph 16.1 above, if the Customer terminates during the Minimum Period of Service, the Customer will pay BT for any parts of the BT Managed Cloud Security (Zscaler) Service that were terminated during the Minimum Period of Service, a compensation, equal to:

(a) 100 per cent of the Recurring Charges for any remaining months of first twelve (12) Months of the Minimum Period of Service; and
(b) 50 per cent of the Recurring Charges for the remaining months of the Minimum Period of Service, other than the ones set out in Paragraph 16.2(a) above; and
(c) any waived Installation Charges.

16.3 In the event the BT Managed Cloud Security (Zscaler) Service is early terminated during a Renewal Period the same termination fees shall apply.

17 Limitations of Liability

In variance of the limitation of liability in the General Terms and Conditions of the Agreement, the total liability of either Party to the other under or in connection with this Schedule shall not exceed 125% of the total of all net-Charges paid for BT Managed Cloud Security (Zscaler) Services.

18 Service Levels

18.1 **Availability Service Level**

18.1.1 From the Operational Service Date, BT will provide the BT Managed Cloud Security (Zscaler) Service with a target availability of 99.999% of the total hours during every month the Customer uses the BT Managed Cloud Security (Zscaler) Service.

18.1.2 the Availability Service Level is a ratio of the number of Transactions and Sessions processed by the BT Managed Cloud Security (Zscaler) Service in any calendar month, against the number of qualified Transactions and Sessions that should have been processed.

18.1.3 The Supplier will measure the number of Transactions and Sessions. The following Transactions and Sessions will not be taken into account for the Availability Service Level:

(a) Transactions and Sessions that are encrypted, encapsulated, tunnelled, compressed, modified from their original form for distribution; and/or

(b) Transactions and Sessions that have product license protection; and/or

(c) Transactions and Sessions that are under the direct control of the sender (e.g. password protected).); and/or

(d) Transactions and Sessions that occur during Zscaler scheduled maintenance periods, as posted on the Trust Portal: https://trust.zscaler.com/.

18.1.4 For the avoidance of doubt, no Availability Service Level or Availability Service Credit shall be offered in connection with the Eagle-i Service.

18.1.5 Availability Service Credits

If the Availability Service Level is not met, the Customer may claim an Availability Service Credit as follows:

Percentage of Transactions and Sessions Processed During a Month	Availability Service Credit
>= 99.999%	No Availability Service Credit applicable.
< 99.999% but >= 99.99%	(3 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Availability Service Credit claim.
< 99.99% but >= 99.00%	(7 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Availability Service Credit claim.
< 99.00% but >= 98.00%	(15 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Availability Service Credit claim.
< 98.00%	(30 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Availability Service Credit claim.

18.2 **Latency Service Level**

18.2.1 From the Operational Service Date, BT will provide the BT Managed Cloud Security (Zscaler) Service to process:

(a) for any other, Transactions and Data Packets with an average latency over a calendar month of 100 milliseconds or less for the 95th percentile of traffic.

18.2.2 The Latency Service Level will only apply to Transactions if:

(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) there are a reasonable number of Transactions per User Subscription (based on the Supplier's cloudwide average).

18.2.3 BT (via the Supplier) will measure the processing of content from when the Supplier's proxy receives the content to the point when the Supplier's proxy attempts to transmit the content.

18.2.4 For the avoidance of doubt, no Latency Service Level or Latency Service Credit shall be offered in connection with the Eagle-i Service.

18.3 Virus Capture Rate Service Level

18.3.1 From the Operational Service Date, BT will provide the BT Managed Cloud Security (Zscaler) Service with a target of capturing 99.999% of Known Viruses over a calendar month.

18.3.2 The Virus Capture Rate Service Level applies to the BT Managed Cloud Security (Zscaler) Service

18.3.3 The Virus Capture Rate Service Level applies only if:

(a) the Customer utilises the BT Managed Cloud Security (Zscaler) Service in accordance with the recommended anti-virus settings on the Customer user interface; and

(b) a Known Virus contained in a Transaction received through the BT Managed Cloud Security (Zscaler) Service has been activated within the Customer's systems, either automatically or with manual intervention.

18.3.4 In the event that BT (or the Supplier) detects but does not stop a Known Virus, the BT will promptly notify the Customer, providing sufficient information to enable the Customer to identify and delete the Known Virus. If the Customer does not promptly act on this information the Service Credit may be invalidated.

18.3.5 In the event of such BT notification and a subsequent action by the Customer results in a prevention of infection, the Virus Capture Rate Service Level will not apply.

18.3.6 BT (via the Supplier) will calculate the Virus Capture Rate by dividing the virus-infected Transactions blocked by the total virus-infected Transactions received by the BT Managed Cloud Security (Zscaler) Service on the Customer's behalf.

18.3.7 For the avoidance of doubt, no Virus Capture Rate Service Level or Virus Capture Rate Service Credit shall be offered in connection with the Eagle-i Service.

18.3.8 Virus Capture Rate Service Credits. If the Virus Capture Rate Service Level is not met, the Customer may claim a Virus Capture Rate Service Credit as follows:

Virus Capture Rate	Virus Capture Service Credit
>= 99.999%	No Virus Capture Rate Service Credit available.
< 99.999% but >= 99.00%	(7 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Virus Capture Rate Service Credit claim.
< 99.00% but >= 98.00%	(15 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Virus Capture Rate Service Credit claim.
< 98.00%	(30 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Virus Capture Rate Service Credit claim.

18.4 Zscaler Private Access Service Level

18.4.1 From the Operational Service Date, BT will provide Zscaler Private Access with a target availability of 99.999% of the total hours during every month the Customer uses Zscaler Private Access ("**Zscaler Private Access Service Leve**l").

18.4.2 Zscaler Private Access Service Credits. If the Zscaler Private Service Level is not met, the Customer may claim a Zscaler Private Service Credit as follows

Percentage of Transactions and Sessions Processed During a Month	Zscaler Private Access Service Credits
>= 99.999%	No Zscaler Private Access Service Credit applicable.
< 99.999% but >= 99.99%	(3 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Zscaler Private Access Service Credit claim.
< 99.99% but >= 99.00%	(7 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Zscaler Private Access Service Credit claim.
< 99.00% but >= 98.00%	(15 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Zscaler Private Access Service Credit claim.

Percentage of Transactions and Sessions Processed During a Month	Zscaler Private Access Service Credits
< 98.00%	(30 / 30) x the monthly Recurring Charge for the relevant part of the BT Managed Cloud Security (Zscaler) Service in the month immediately preceding the Incident giving rise to the Zscaler Private Access Service Credit claim.

18.4.3 For the avoidance of doubt, no Zscaler Private Access Service Level or Zscaler Private Access Service Credit shall be offered in connection with the Eagle-i Service.

18.5 **On Time Delivery Service Level**

In the event the Customer has ordered Foundation Plus or Premium, BT will provide following additional Service Level for On Time Delivery:

18.5.1 BT will use reasonable endeavours to deliver the BT Managed Cloud Security (Zscaler) Service on or before the Customer Committed Date as agreed with the Customer. The On-Time Delivery Service Level does not apply to upgrades or changes to the BT Managed Cloud Security (Zscaler) Service, unless these have a new agreed delivery date, in which case the Customer Committed Date will be that agreed delivery date. BT may expedite delivery of the BT Managed Cloud Security (Zscaler) Service for operational reasons or in response to a request from the Customer, but this will not revise the Customer Committed Date.

18.5.2 On Time Delivery Service Credits. If BT does not meet the On Time Delivery Service Level, the Customer may claim a Service Credit equal to EUR 100.00 per Business Day late, calculated from the agreed Customer Committed Date until the Operational Service Date of such BT Managed Cloud Security (Zscaler) Service, and this up to a maximum amount equal to the Installation Charges for that BT Managed Cloud Security (Zscaler) Service.

19 Requests for Service Credits

19.1 To qualify for Service Credits, and before any Service Credits can be applied, the Customer must make a claim within 25 days after the end of the month in which the **BT Managed Cloud Security (Zscaler) Service** underperformed or where a longer time period is required by mandatory local law then the shortest period that can be applied.

19.2 Upon receipt of a valid request for Service Credits, BT will review the validity of the request and:

(a) BT will carry out these reviews on a monthly basis;
(b) if the request for Service Credits was not valid, BT will notify the Customer accordingly;
(c) if the request for Service Credits is valid, BT will notify the Customer of the Service Credit due:
(d) BT will deduct the Service Credits from the Customer's invoice within two (2) billing cycles of the request being received; and
(e) following expiry or termination of the BT Managed Cloud Security (Zscaler) Service where no further invoices are due to be issued by BT, BT will pay the Customer Service Credits within two (2) months.

19.3 The following is an example of Service Credit calculation where:

(a) the monthly Recurring Charge is EUR 50,000 per month; and
(b) the Service Credit due is three (3) days.
(c) BT will provide a credit on the next invoice of EUR 50,000/30 days x 3 days i.e. EUR 5,000.

19.4 Service Credits for all Service Levels will be aggregated and are available up to a maximum amount equal to 100 per cent of the monthly Recurring net-Charge for the affected BT Managed Cloud Security (Zscaler) Service.

19.5 All Service Levels and Service Credits will be calculated in accordance with information recorded by, or by the Supplier on behalf of, BT.

19.6 The following items are excluded from the calculation of Availability Service Levels:

(a) Customer's network is not forwarding traffic to the BT Managed Cloud Security (Zscaler) Service; or
(b) an intermediate ISP (other than the BT Managed Cloud Security (Zscaler) Service's direct ISP(s)) is not delivering traffic to the BT Managed Cloud Security (Zscaler) Service; or
(c) the drop in Transactions and Sessions is due to a policy change requested by the Customer; or
(d) it is not technically possible to scan the Customer's traffic; e.g. items that

(ii) are encrypted, encapsulated, tunnelled, compressed, modified from their original form for distribution; and/or
(iii) have product license protection; and/or
(iv) are under the direct control of the sender (e.g. password protected).

19.7 The Service Levels will not apply:

(a) where the Customer network is not properly configured on a 24 hours a day x 7days per week x 365 days per year basis in a manner that allows the Customer to make use of the Supplier's redundant global infrastructure that is made available as part of the BT Managed Cloud Security (Zscaler) Service. BT will communicate this to the Customer at the time it commissions the BT Managed Cloud Security (Zscaler) Service;

(b) during any trial period of the BT Managed Cloud Security (Zscaler) Service;

(c) to failures due to any Force Majeure Event;

(d) if the Customer causes a delay or does not provide any requested information in accordance with any agreed timescales;

(e) to any Incident not reported in accordance with this Schedule; or

(f) if the Customer is in breach with the terms of the Agreement.

(g) if the Incident was a result of Simple Changes implemented by the Customer through Co-Management Service Option.

19.8 Without forfeiting any other rights the Customer has under the Agreement, it acknowledges that Availability Service Credit claims is the only Customer remedy if BT and/or the Supplier fails to meet the applicable Availability Service Level.

20 Data Protection

20.1 Applicable terms. The Parties agree that it is anticipated that BT and the Supplier may receive or process Personal Data on behalf of the Customer as a Data Processor in connection to the Service or as a result of the provision of this Service. Any Customer Data is subject to the 'Data' clause as set out in the Agreement.

20.2 The nature and purpose of the Processing of Customer Personal Data by BT;

(a) The BT Managed Cloud Security (Zscaler) Service allows the Customer to set rules by which URLs are blocked and web content is filtered on its IT systems. The software itself is provided by the Supplier and hosted on that Supplier's public cloud infrastructure, with no access to underlying information possible for BT. The Customer may select to have its transaction logs stored in the EEA and Switzerland using the following hub data centers: (1) Interxion Deutschland GmbH in Frankfurt, Germany; (2) Equinix (Netherlands) B.V. in Amsterdam, Netherlands; and (3) Equinix (Switzerland) GmbH in Zurich, Switzerland. The following URL provides a full overview of Sub-Processors used by the Supplier: https://www.zscaler.com/legal/subprocessors.

(b) With the BT Managed Security Service overlay, BT will have access through the online portal to a log of the Customer IP addresses and MAC addresses, together with attempted URL or website visits by those addresses, in order to provide reports to the Customer. BT has no access to data other than within this portal.

20.3 The types of Customer Personal Data Processed by BT or its Sub-Processors or the Customer will be:

- website or IP address;
- name;
- address;
- telephone number;
- email address;
- job title;
- company name;
- contact records;
- usage records (call, internet or router logs);
- transaction logs, and
- identity management - user profiles.

20.4 The Customer Personal Data will concern the following categories of Data Subjects:

- the Customer employees;
- the Customer's customers or third parties; and
- any Data Subject (as controlled by the Customer).

Customer [Include Complete Customer name]	BT Global ICT Business Spain, S.L.U.
Signed: (Authorised representative)	Signed: (Authorised representative)
(Name)	Paul Rhodes
Legal representative	Legal representative

Appendix 1 to BT Managed Cloud Security (Zscaler) Service

Zscaler Acceptable Use Policy

This Acceptable Use Policy ("AUP") outlines acceptable uses of Zscaler services and products ("Products"). This AUP prohibits uses and activities involving the Products that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Products by others. For example, these prohibited uses and activities include using the Products to:

Conduct and Information Restrictions

- Undertake or accomplish any unlawful purpose. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation;
- Upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Products or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner;
- Transmit unsolicited bulk or commercial messages commonly known as "spam;"
- Send very large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send very large messages or files that disrupts a server, account, blog, newsgroup, chat, or similar service;
- Participate in the collection of very large numbers of e-mail addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including "spyware") designed to facilitate this activity;
- Falsify, alter, or remove message headers;
- Impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, "phishing");

Technical Restrictions

- Access any other person's computer or computer system, network, software, or data without his or her knowledge and consent; breach the security of another user or system; or attempt to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so;
- Use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is strictly prohibited;
- Copy, distribute, or sublicense any proprietary software provided in connection with the Products by Zscaler;
- Distribute programs that make unauthorized changes to software (cracks);
- Alter, modify, or tamper with the Products or permit any other person to do the same who is not authorized by Zscaler;

Network and Usage Restrictions

- Restrict, inhibit, or otherwise interfere with the ability of any other entity, to use or enjoy the Products, including posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information;
- Restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation to the Products or any Zscaler (or Zscaler supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any Zscaler (or Zscaler supplier) facilities used to deliver the Products;
- Interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host.

ZSCALER RESERVES THE RIGHT TO NOTIFY ITS CUSTOMERS OF ANY INFORMATION THAT AFFECTS THE SECURITY OF THE PRODUCTS.

If you have any questions about this AUP, please contact Zscaler as follows:

Zscaler, Inc.
ATTN: Legal Department
110 Rose Orchard Way
San Jose, CA 95134, USA
Email: contracts@zscaler.com

Simple and Complex Changes

Note: As any change not qualified in below table as "Simple" will be a Complex Change; the below listed Complex Changes are non-exhaustive examples.

Simple (also known as SSRs - Simple Service Requests)

Change	Mechanism for Requesting Change
Update URL Category	BT Security Change Manager
Change to Resolve Incident/s	BT Security Change Manager
Change URL Filtering Rules	BT Security Change Manager
SSL Inspection Rules	BT Security Change Manager
Add/modify Administrator account (ZIA)	BT Security Change Manager
Reset Administrator account password (ZIA)	BT Security Change Manager
Remove Administrator account	BT Security Change Manager
Security Exceptions Bypass Inspection	BT Security Change Manager
Change Malware Protection Settings	BT Security Change Manager
Change Advanced Threat Protection Settings	BT Security Change Manager
File Type Control	BT Security Change Manager
Browser Control	BT Security Change Manager
Sandbox Settings	BT Security Change Manager
Add User account (ZIA ONLY)	BT Security Change Manager
Modify/remove User account (ZIA ONLY)	BT Security Change Manager
Add/modify/remove User Group SAML Attributes	BT Security Change Manager
ZCC (Mobile Portal) - add/modify Linux profile - no Tunnel 2.0 config	BT Security Change Manager
ZCC (Mobile Portal) - add/modify MacOS profile - no Tunnel 2.0 config	BT Security Change Manager
ZCC (Mobile Portal) - add/modify Windows profile - no Tunnel 2.0 config	BT Security Change Manager
ZCC (Mobile Portal) - add/modify Tunnel 2.0 config	BT Security Change Manager
ZCC (Mobile Portal) - add/modify Android profile	BT Security Change Manager
ZCC (Mobile Portal) - add/modify IOS profile	BT Security Change Manager
ZCC (Mobile Portal) - remove profile	BT Security Change Manager
Sublocation - add/modify/remove (ZIA ONLY)	BT Security Change Manager
Add Application Segment	BT Security Change Manager
Existing Application Segment - add/remove application or ports	BT Security Change Manager
Access Policy - add/modify/remove	BT Security Change Manager
Timeout Policy - add/modify/remove	BT Security Change Manager
Add/modify Administrator account (ZPA)	BT Security Change Manager

Reset Administrator account password (ZPA)	BT Security Change Manager
Client Forwarding Policy - add/modify/remove	BT Security Change Manager
Change To Rebuild Failed App Connector/s	BT Security Change Manager

Complex Non-Contract Affecting

Change	Mechanism for Requesting Change
Extend MCS service to a new site	My Account
Identity integration assistance	My Account
Policy definition assistance (L)	My Account
Policy definition assistance (M)	My Account
Policy definition assistance (S)	My Account
Support for Customer SSL Decryption (L)	My Account
Support for Customer SSL Decryption (M)	My Account
Support for Customer SSL Decryption (S)	My Account
Traffic Forwarding (L)	My Account
Traffic Forwarding (M)	My Account
Traffic Forwarding (S)	My Account

Complex Contract Affecting

Change	Mechanism for Requesting Change
Addition of SKU feature from Zscaler	Managed by the Account Team
Addition of users	Managed by the Account Team
Additional feature from BT	Managed by the Account Team
Cease/Downgrade Zscaler (inc. calculation of termination charges)	Managed by the Account Team
Change contract length	Managed by the Account Team
Foundation - move from SIP to Professional	Managed by the Account Team
Move of GSM Service Tiers - move from Foundation to Foundation Plus or Premium and Foundation Plus to Premium	Managed by the Account Team