BT Managed Security (Zscaler) Service Schedule
Part B – Service Description

Section A The Service

1. STANDARD COMPONENTS OF THE SERVICE

BT will provide the Customer with the following Services in accordance with the details as set out in the Order:

1.1 Supplier Services. At least one of the following security modules of the Supplier will be provided and supported by BT:

Zscaler Services	Description
Zscaler Internet Access ("**ZIA**")	ZIA is a software-based cloud service that allows the Customer to select various security options to be applied at cloud data centres across the world to protect the Customer's Internet traffic.
Zscaler Private Access ("**ZPA**")	ZPA is a software-based cloud service that provides secure remote access to internal applications for the Customer's Users, regardless of their Location, and without the Users being on the Customer's network.
Zscaler Digital Experience ("**ZDX**")	ZDX is a software-based cloud service that allows the Customer to set rules for which User experience insights can be understood for endpoints, applications and network.
Zscaler Client Connector ("**ZCC**")	ZCC is a client application allowing access to the Service through certain mobile operating systems and computers.

1.2 Supplier Software: This is Supplier Software for use during the Subscription Term for the Users, and/or Locations as set out in the Order for the Customer to download and install on the User devices.

1.3 Supplier Portal: The Supplier provided secure portal provides BT and the Customer with a right to access and use the Supplier's web-based user interface. The Supplier Portal is an administrative portal for creating and managing security policies, digital experience monitoring configuration, reporting and analysing traffic. The Supplier Portal gives the Customer a primary Administrator account that will allow the Customer to create multiple Administrators and enables the Customer to:

1.3.1 review statistics of all Malware that is stopped and other Internet content that is blocked;

1.3.2 create access restrictions and apply these to specific Users or groups of Users;

1.3.3 customise browser alert pages seen by Users when web-access is denied;

1.3.4 manage rules for User experience insights;

1.3.5 update administration details for real-time email alerts;

1.3.6 use the Supplier Portal to track User experience monitoring, perform troubleshooting and self-serve subject to licence to improve productivity issues;

1.3.7 configure and schedule automated system auditing and reporting;

1.3.8 view any Supplier Planned Maintenance provided for geographic region(s) and Supplier registered incidents (not real time) by using the Supplier Portal - https://trust.zscaler.com/zscaler.net

1.3.9 view advisory information published by the Supplier regarding any new evasion techniques, vulnerabilities discovered and addressed by the Supplier.

The Customer data will be retained on the Supplier Portal for a period of six months.

1.4 **BT Portal:** Provides a secure mechanism for service requests and incident management.

1.5 **BT Support**. BT will provide the Foundation Graded Service Tier as standard. The features of Foundation are as follows:

BT Support	Description - Foundation Features
Implementation Support	BT is responsible for managing the Order on behalf of the Customer - including the purchase of licences from the Supplier. The Supplier Portal link(s) are sent directly to the Customer to administer the solution fully. The Customer will provide BT with an admin account in order for BT to provide in-life support. The Customer will have access to the BT Portal to raise Incidents.
Reactive Incident Management	BT will provide only reactive support on any Incidents raised regarding an outage, security issue or performance degradation on the Supplier platform as BT has no real time access to the Supplier platform.
BT Service Desk - 1st Line Reactive Incident Management	The BT Service Desk is responsible for managing Incidents raised via the BT Portal by the Customer. Initial triage of the issue is carried out by using structured questions to capture all of the relevant details. Where necessary, if the issue cannot be resolved by the Service Desk, an Incident will be raised with the BT Global Security Operations Centre ("**GSOC**"). The Customer can access the BT Portal for progress updates and to respond to any requests for information BT asks for in order to help resolve the issue. Once the Incident is resolved, an update will be posted on the BT Portal and the Incident closed following confirmation from the Customer.
BT Global Security Operations Centre support - 2nd Line Reactive Incident Management	The GSOC is responsible for managing Incidents raised by the BT Service Desk which can't be resolved at 1st Line. The GSOC will carry out in-depth analysis, which will include logging on to the Supplier Portal to troubleshoot, check for best practices, etc. Where necessary, if the GSOC cannot resolve the issue, an Incident ticket will be raised with the Supplier.
Reporting	The Customer will have access to the Supplier Portal to view the dashboards and view capabilities offered by the Service. Reports available can be exported and/or scheduled, based on requirements.

Further details of these BT support services are set in Paragraph 8 of this Part B.

2. SERVICE OPTIONS

BT will provide the Customer with any of the following chargeable options as set out in any applicable Order and in accordance with the details as set out in that Order:

2.1 **Optional BT Support Services**. The Customer may select the Foundation Plus and Premium Graded Service Tiers. In addition to the standard features as set out in Paragraph 1.5, the features of Foundation Plus and the Premium Graded Service Tiers are as follows:

BT Support	Description

Implementation Support	BT will provide resources to manage the implementation of the Order, including an order manager to complete the order to the Supplier and BT system-related tasks. A project manager will be provided to oversee and coordinate resources to configure and test the Supplier Portal. When the configuration is completed, there will be a handover to the in-life operational teams.
Simple Service Requests ("**SSRs**")	In accordance with the Service Request Management Process set out in Paragraph 8.5; the Customer may request SSRs per Zscaler product which will be available via the catalogues on the BT Portal. The default settings per month are as follows: For Foundation Plus: • 8 SSR changes per Zscaler Service per month. For Premium: • 10 SSR changes per Zscaler Service per month.
Complex Service Requests ("**CSRs**")	The Customer can request help from BT via the BT Portal for requests that are complex and require technical support to be provided. These are reviewed on an individual case basis and the Customer will be informed of the applicable charges to carry out the specific CSR requested. The Charges and Service details will have to be agreed on an Order before any CSR is implemented.
Co-Management	BT will provide the Customer with a Role Based Account Control Profile ("**RBAC Profile**") for up to a maximum of 5 authorised nominated Users on the Supplier Portal. Users of the RBAC Profile will have restricted access to implement SSR's. BT will provide the Customer with a separate user guide setting out details how to manage SSR's.
Reporting	BT will provide reports with regards to Incident Management, SSRs and CSRs. For Foundation Plus: • quarterly For Premium • monthly there will be a review and report to the Customer as further detailed in Paragraph 8.4.2 of this Part B.
Security Optimisation Manager ("**SOM**")	The SOM will provide security-specific technical support and will review and make any recommendations on optimizing the Service. This will ensure best practice.
Service Manager ("**SM**")	The SM is a value-add option that can be selected if the Customer does not already have a Customer service manager for other BT services. The primary role of the SM is: • providing regular reporting on the Incident and service request management functions • updating the Customer Handbook; and • reviewing any service improvement initiatives.
Proactive Management	For ZDX, BT will set-up any applications, and network-based alerts to be shared with the Customer and BT for key services. For Foundation Plus: • up to 5 alerts will be created,

	For Premium • up to 10 alerts will be created.
BT Eagle-i	BT Eagle-i is a tool providing enhanced Security Incident alerts, which contains additional detail on the reported Security Incident allowing BT to provide improved recommended mitigation or corrective action to the Customer. Depending on the Graded Service Tier selected, the BT Eagle-i Service option provides various management options as set out on the Order.

2.2 **Optional Supplier Services**. The Customer may order from BT one or more additional features offered by the Supplier in addition to ZIA, ZPA or ZDX to enhance or extend the capabilities of the Supplier Services (called "**Zscaler SKUs**"). The available Supplier Service options from BT are set out in the Customer Handbook. The Zscaler SKUs may change from time to time due to changes in the Supplier's offering.

3. SERVICE MANAGEMENT BOUNDARY AND SERVICE LIMITATIONS.

3.1 BT's responsibility to provide and manage the Service up to and including the following service management boundary:

3.1.1 The standard Service elements as set out in Paragraph 1; including the Supplier Portal/s where access is managed by BT and the BT Portal;

3.1.2 Any ordered optional Service elements set out in Paragraph 2; whereby for the Service elements forming part of a Graded Service Tier level this limited to the optional Service elements forming part of the ordered Graded Service Tier.

3.2 Paragraph 3.1 constitutes the "**Service Management Boundary**."

3.3 BT will have no responsibility for the Service outside the Service Management Boundary.

3.4 BT does not make any representations, whether express or implied, about:

3.4.1 whether the Service will operate in combination with any Customer equipment or other equipment and software; and

3.4.2 the ability of the Service to detect and mitigate all Unknown Viruses, malicious threats or attacks from the Internet.

4. ENABLING SERVICE

4.1 The Customer will have the following services in place that are necessary for the Service to function:

4.1.1 Internet connectivity between the User Devices and cloud infrastructure provided by the Service and the Supplier platform;

4.1.2 Customer equipment and User Devices; and

4.1.3 Applications for any User experience performance monitoring.

(the "**Enabling Service**")

5. COMMISSIONING OF THE SERVICE

5.1 Before the Operational Service Date, BT will:

5.1.1 deliver and configure the Service as set out in the Order;

5.1.2 conduct a series of standard tests on the Service to ensure that it is configured correctly;

5.1.3 connect the Service to each Enabling Service;

5.1.4 on the date that BT has completed the activities in this Paragraph 5.1, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

6. ACCEPTANCE TESTS

6.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("**Acceptance Test Period**").

6.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

6.3 Subject to Paragraph 6.4, the Operational Service Date will be the earlier of the following:

6.3.1 the date the Customer confirms or BT deems acceptance of the Service in writing in accordance with Paragraph 6.2;

6.3.2 the date of the first day following the Acceptance Test Period; or

6.3.3 the date the Customer starts to use the Service.

6.4 If, during the Acceptance Test Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Supplier Terms

7. EULA

The applicable EULA will be: https://www.zscaler.com/legal/end-user-subscription-agreement

Section C Service Management

8. SERVICE MANAGEMENT

8.1 Technical Incidents

8.1.1 Where the Customer or BT becomes aware of a Technical Incident:

(a) it will be reported to the BT Service Desk;

(b) BT use structured questions to record the details of the Technical Incident. The BT Service Desk will log the Technical Incident in BT's standard Incident management system and generate an Incident ticket;

(c) BT will inform the Customer when it believes the Technical Incident is cleared and will close the Incident Ticket when:

(i) the Customer confirms that the Technical Incident is cleared within 24 hours after having been informed; or

(ii) if BT is unable to reach the Customer to confirm Technical Incident resolution, BT will attempt to contact the Customer three times in total, at regular intervals, before automatically closing the Technical Incident ticket.

(d) If the Customer confirms that the Technical Incident is not cleared within 24 hours after having been informed, the ticket will remain open, and BT will continue to work to resolve the Technical Incident.

8.2 Security Incidents

8.2.1 When BT becomes aware of a Security Incident related to the Service, the GSOC will be assigned to work on the Security Incident and the BT Service Desk will provide updates to the Customer in line with the service targets associated with the priority. Updates will be

communicated via the BT Portal and with any agreed Customer contacts associated with the Security Incident.

8.2.2 When the Customer reports a Security Incident to BT, BT will log the Security Incident and carry out an initial triage of the issue by using structured questions to capture all of the relevant details. Where necessary, if the BT Service Desk cannot resolve the issue the BT Service Desk will raise a Security Incident to the GSOC so they can address more complex cases.

8.2.3 The GSOC is responsible for managing Security Incidents raised by the BT Service Desk for more in-depth analysis to be carried out, which includes logging on to the Supplier Portal/s to troubleshoot, check for best practices, etc.

8.3 Technical and Security Incidents additional terms:

8.3.1 The Customer will ensure that any Incident notification includes all relevant and available information at the time of contacting BT.

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

8.4 Reviews and reporting

8.4.1 Foundation

(a) Reporting is available to the Customer as part of self-service directly on the Supplier Portal.

(b) The Customer will be responsible for administering the Service in life. Incidents can be raised using the BT Portal and additional professional services can be purchased by the Customer if required.

8.4.2 Foundation Plus

(a) Where the Customer has selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a quarterly basis a review on the technical performance of the Service and send a report to the Customer or discuss at review meetings with the following actions:

(i) a review focusing on the performance of the Service; and

(ii) a review of the Customer's security policy(ies) and or Digital Experience Monitoring (if ordered) focusing on the effectiveness of the rules applied to the Customer's security policy(ies) and the need to fine tune or amend the rules of the Customer's security policy(ies) or recommendations on the User experience set up.

8.4.3 Premium

(a) Where the Customer has selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a monthly basis a review on the technical performance of the Service and send a report to the Customer or discuss at review meetings with the following actions:

(i) a review focusing on the performance of the Service; and

(ii) a review of the Customer's security policy(ies) and or Digital Experience Monitoring focusing on the effectiveness of the rules applied to the Customer's security policy(ies) and the need to fine tune or amend the rules of the Customer's security policy(s); or recommendations on the user experience set up.

8.5 Service Request Management process

8.5.1 BT will implement changes to the Customer's security policy(ies) in response to Customer requests, subject to the following process:

(a) BT will provide secure access to the BT Portal to all pre-agreed and authorised Customer contacts to enable service requests to be submitted;

(b) SSRs are upgrades and modifications needed because of planned developments and security improvements. SSRs will be executed subject to the Customer's approval and in accordance with the timing agreed with the Customer. The initial SSRs are set out on the Order which may be amended from time to time depending on changes by the Supplier subject to BT providing notice to the Customer and, where any changes may have a material impact on the Customer, the Customer's approval will be sought; and

(c) SSRs are limited to the quantity per month depending on the Graded Service Tier level ordered by the Customer. If the Customer requires additional SSRs a maximum of 15 per month can be ordered at an additional charge.

8.5.2 Where the Customer raises SSRs more frequently than the allowance; 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 SSRs at the rate as set out in the Order.

8.5.3 BT will communicate the status of all service requests on the BT Security Portal for a period of six months.

8.5.4 The Customer will ensure that any authorised Customer contact with access to the BT Security Portal will not submit any unauthorised requests.

8.6 Co-Management

8.6.1 If the Customer orders Co-Management:

(a) BT will provide the Customer with a separate user guide setting out details how to manage SSRs; and

(b) if a SSSR implemented by any User using the RBAC Profile has resulted in an Incident as notified by the Customer in accordance with paragraph 8.1, BT will provide assistance to resolve the Incident using the audit and logging capability on the Supplier Portal to support any root cause analysis undertaken to confirm this.

8.7 Service targets

8.7.1 Service Care target response times and follow-up

(a) The Foundation Graded Service Tier support provides support as set out in the table below.

(b) The Customer must have a dedicated employee who is available by phone with the necessary access to assist in troubleshooting. If an employee is not available, the Customer will agree with BT on a timeframe for updates.

		Incident Stage			
Priority	**Description**	**Initial Response**	**Next Response**	**Further Responses**	**Target Restoration**
P1	One or more core Service components are completely unavailable or one or more core business functions are completely unable to be performed. This would typically affect all Users for this Service; e.g. where the Supplier Portal is	Customer will be informed that BT is dealing with their Incident within 15 minutes of receiving it (either via an alert or by the Customer advising us)	First update within 30 minutes from the Incident ticket being opened	Every 60 minutes	4 hours

	inaccessible, or the Supplier cloud platform core components are completely unavailable.				
P2	A partial interruption or impairment to the Service, which cannot be mitigated, or core business functions can be performed but in a reduced capacity.	Customer will be informed that BT is dealing with their 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	Minor or intermittent impact to the Service, the majority of Users are able to access the Service, however a small number of Users may be impacted.	N/A	First update within 4 hours from the Incident ticket being opened	Every 4 hours	24 hours
P4	Very minor or no business impact, such as a single User having minor localised issues but core business functions can be carried on as normal.	N/A	First update within 24 hours from the Incident ticket being opened	Every 24 hours	48 hours