BTnet Security
Annex to the BTnet Service Schedule

Part A – The BTnet Security Service

1 Service Summary

This Annex to the BTnet Service Schedule (the **"Schedule"**) will only apply where the Customer has selected BT Equipment as part of the BTnet Service and placed an Order for the BTnet Security Service. The BTnet Security Service is for use with a single BTnet Internet connection from Customer Sites in the UK and does not provide any site to site VPN capability.

2 Standard Service Components

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

2.1 **Managed Installation**

BT will coordinate the BTnet Security Service installation and commissioning, liaising with the Customer, installers and equipment suppliers as appropriate. BT will administer all activities remotely.

2.2 **Service Performance Reports**

BT will grant the Customer access to reporting functionality for key BTnet Security Service performance metrics and for some security-related events.

3 Service Features

BT will provide the Customer with the following service features that are only available in the UK:

3.1 **Layer 3 Firewall**

3.1.1 BT will configure the Customer's firewall to allow outbound traffic. All inbound traffic will be blocked by default.

3.1.2 BT will carry out configuration changes to the Customer's Layer 3 Firewall on request, where necessary.

3.1.3 If BT agrees a request from the Customer to alter its firewall policy, the Customer accepts responsibility for these changes.

3.1.4 BT will provide a standard security configuration template for the Customer's BTnet Security Service the Customer will own and will be responsible for this configuration, including any changes or additions that it asks BT to make to its configurations and policies.

3.2 **Layer 7 Firewall with Application Control**

3.2.1 Layer 7 Firewall enables, upon request, creation of firewall rules to block specific web-based services, websites, or types of websites without having to specify IP addresses or port ranges. BT will block certain categories by default when BT accepts the Order.

3.2.2 The Customer may request BT to provide the list of blocked application categories and all additional available categories.

3.2.3 BT is not responsible for how the applications are categorised, the regularity of update or for evaluating which applications fall under each category.

3.2.4 The Customer may request BT to add or remove available application categories.

3.2.5 The Customer will accept responsibility for the configuration and any changes made to access applications and any increased risk of being exposed to malicious content.

3.3 **Content Filtering**

3.3.1 BT will block certain categories of websites by default when BT accepts the Order. The Customer may request BT to provide the list of blocked categories ("**Blocked Categories List**") and all additional available categories.

3.3.2 BT will provide the Customer with Content Filtering in two modes: the full list mode or the top sites only mode.

3.3.3 BT will set the Customer's default configuration to the full list mode for better coverage. In this mode, the Customer's request for a URL that is not in the list of top sites only will cause the appliance to look the URL up in a cloud-hosted database. The Customer acknowledges that this may have a noticeable impact on browsing speed and performance when visiting a Site for the first time. The result will then be

cached locally. Over time, the full list performance should approach the speed of the top sites only mode.

3.3.4 On the Operational Service Date, the Customer may choose to switch setting to the top sites only. In this mode, the list of top sites in each of the blocked categories will be cached locally on the appliance. The Customer's request for a URL that is not in the top sites only list will always be permitted (as long as they are not in the blocked categories list).

3.3.5 To block access to sites that employ https rather than http the Customer must set the full list. The Customer acknowledges that it is not possible to return an explanatory page to a user where the URL filtering element has blocked an https based website.

3.3.6 The websites and applications captured under these categories are dependent on the Content Filtering System URL categorisation database for CIPA (Children's Internet Protection Act) and IWF (Internet Watch Foundation) compliant content-filtering. Website categories are regularly updated. BT does not take any responsibility for how the websites and applications are categorised or the regularity of updates.

3.3.7 The Customer may request BT to add or remove available categories to restrict or allow the Customer's Users access to categories of websites.

3.3.8 For URL filtering, the Customer may request BT to white list or block particular URL addresses within a category.

3.3.9 The Customer will be responsible for the configuration and any changes made to access to websites and any increased risk of being exposed to malicious web content.

3.4 **Intrusion Detection and Prevention Service**

3.4.1 BT will:

(a) monitor traffic to identify traffic patterns that match known threats, in accordance with the applicable intrusion signature files using Intrusion Detection and Prevention System;

(b) implement this service feature with a default configuration setting, including a standard signature list which works using Intrusion Detection and Prevention System;

(c) not be responsible for evaluating the signatures beforehand;

(d) select the "**balanced**" ruleset as the default detection setting. "**Balanced**" ruleset contains rules that are from the current year and the previous two years, are for vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 9 or greater, and are in one of the following categories:

(i) **Malware-CNC (Command and Control)**: Rules for known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

(ii) **Blacklist**: Rules for URLs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

(iii) **SQL (Structured Query Language) Injection**: Rules that are designed to detect SQL Injection attempts; and

(iv) **Exploit-kit**: Rules that are designed to detect exploit kit activity.

(e) select "**prevention**" as the default configuration setting in the Order. Traffic will be automatically blocked if it is detected as malicious based on the detection ruleset set out in Paragraph 3.4.1(d);

(f) agree to alter the setting from "**prevention**" to "**detection**" or "**disabled**" upon the Customer's request. If "**detection**" mode is selected, the BTnet Security Service will no longer block traffic patterns which match;

(g) known threats and only identify them, and if "**disabled**" mode is selected, no prevention or detection will take place; and

(h) not pro-actively or reactively investigate or act upon detected or prevented threats or attacks.

3.4.2 Use of "Intrusion Prevention" feature may result in false positives where certain applications and traffic flows may cause the feature to block legitimate traffic (e.g. applications not adhering to network communication standards). BT will not be liable if false positives occur and as a result, legitimate traffic is blocked.

3.4.3 If BT agrees a request to alter the parameters for applying new signatures to give a greater or lower sensitivity to attacks, the Customer will be responsible for the outcome of these changes and accept the potential increased risk of false positives (blocks to legitimate traffic) or the increased risk of threats being missed. This includes whitelisting a specific intrusion detection signature or changing the ruleset from 'balanced' to a different mode.

3.5 **Advanced-Malware Protection (AMP)**

3.5.1 BT will:

(a) inspect HTTP file downloads and block or allow file downloads based on their disposition, by using a file reputation based protection engine powered by Cisco AMP; and

(b) determine the disposition of a file as "**clean**", "**malicious**" or "**unknown**" using the threat intelligence retrieved from Cisco AMP.

3.5.2 Files can change disposition based on new threat intelligence e.g. a downloaded file can go from having a "**clean**" to a "**malicious**" disposition. BT will not be responsible for taking any action or for informing the Customer should a file change disposition. BT will only classify the file at the point of inspection.

3.5.3 When traffic is filtered, the URL or ID and the action taken are logged in the portal used by BT.

3.5.4 The Customer may white list specific URL's and files upon request. The Customer may also disable the Cisco AMP service feature entirely upon request.

3.5.5 The Customer will be responsible for the configuration and any changes made to the Cisco AMP service feature and any increased risk of being exposed to malicious content.

3.5.6 Use of Cisco AMP may result in false positives where a file or URL that the Customer deems safe is blocked. BT is not liable when false positives occur and result in legitimate files or URL's being blocked.

3.6 **Security Event Reporting**

3.6.1 BT will:

(a) provide reporting functionality for key Service performance metrics, and for some security-related events.; and

(b) not pro-actively view the Customer's reports and events for security incidents or threats. BT will not pro-actively send the Customer any information regarding security event reporting.

3.6.2 The period over which BT can analyse data is dependent on the capacity of, or the space allocated on, the reporting platform.

3.7 **Security Settings and Configuration**

3.7.1 BT will configure the Customer's compatible BTnet Security Service with a templated set of security policies.

3.7.2 The Customer will own and will be responsible for this templated configuration, including any changes or additions that the Customer asks BT to make to the security configurations and policies.

3.7.3 BT will not vet or assess any changes to the security configuration that the Customer asks to be made.

3.7.4 BT is not responsible for the total security of the Customer's network, User devices, connection or Internet traffic.

3.7.5 BT will make configuration changes, where requested by the Customer using the agreed format and during Business Hours, and complete them by the end of the next Business Day.

3.7.6 BT may charge the Customer for configuration changes to the BTnet Security Service if BT considers that the number or frequency of such changes are excessive. BT and the Customer will agree on pricing for any configuration changes before implementation.

4 Installation and Acceptance

4.1 For Orders placed at the same time as a BTnet Service, BT will aim to install the BTnet Security Service on the same Customer Committed Date that is agreed for the BTnet Service. BT will activate the BTnet Security Service on the same Operational Service Date as the BTnet Service.

4.2 For Orders for BTnet Security Service placed for existing BTnet Service, BT will activate the BTnet Security Service during Business Hours, in three Business Days from acceptance of the Order.

4.3 Before the Operational Service Date and, where applicable, throughout the provision of the BTnet Security Service, BT will configure the BTnet Security Service remotely in accordance with the default security configuration ready for Operational Service Date.

4.4 On the date that BT has completed the activities set out in this Paragraph 4, BT will confirm the Operational Service Date or, if applicable, that the BTnet Security Service is available for performance of any Acceptance Tests as set out in the Support Services Schedule.

5 Minimum Term

5.1 The Minimum Term for the BTnet Security Service will commence from the Operational Service Date and will run co-terminus with the Minimum Term for the BTnet Service.

6 Termination Charges

6.1 The following Termination Charges apply to the BTnet Security Service: an amount equal to 100 per cent of the Regular Charges for all other remaining months of the first 12 months of the Minimum Term; and an amount equal to 50 per cent of the Regular Charges for all other remaining months of the Minimum Term.

7 EULA

7.1 BT will only provide the BTnet Security Service if the Customer has entered into the EULA with the supplier in the form set out at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/meraki-seula.pdf .

7.2 The Customer will observe and comply with the EULA for all any use of the applicable Software.

7.3 If the Customer does not comply with the EULA, BT may restrict or suspend the BTnet Security Service upon reasonable Notice, and:

(a) the Customer will continue to pay the Charges for the BTnet Security Service until the end of the Minimum Term; and

(b) BT may charge a re-installation fee to re-start the BTnet Security Service.

7.4 The Customer will enter into the EULA for its own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between the Customer and the supplier and the Customer will deal with the supplier with respect to any loss or damage suffered by either of the Customer as such loss or damage will not be enforceable against BT.

7.5 Where the EULA is presented in a 'click to accept' function and the Customer requires BT to configure or install Software on the Customer's behalf, BT will do so as the Customer's agent and bind the Customer to the EULA.

8 Invoicing

8.1 Invoicing will be as set out in the BTnet Service Schedule or Contract.

Part B – Service Delivery and Management

9 BT's obligations

9.1 **Service Delivery and Commissioning of the BTnet Security Service**

9.1.1 Before the Operational Service Date and, where applicable, throughout the provision of the BTnet Security Service, BT will configure the BTnet Security Service remotely in accordance with the default security configuration ready for Operational Service Date.

9.2 **During Operation**

On and from the Operational Service Date, BT:

9.2.1 will work with the relevant supplier to restore the BTnet Security Service as soon as practicable if the Customer reports an Incident; and

9.2.2 will not be liable in the event that Software updates from the supplier used to identify and control the Customer's network traffic (including malware signatures, URL categories or application definitions) contain errors or omissions, beyond making appropriate corrections (where reasonably possible) as soon as reasonably practical.

9.3 **The End of the Service**

On the date of termination of the BTnet Security, BT will:

9.3.1 terminate any rights of access to the relevant Software and stop the BTnet Security Service; and

9.3.2 not have any responsibility for securing the Customer's Internet connection and will not be liable for the increased risk the Customers exposes themselves to.

10 Customer obligations

10.1 **BTnet Security Delivery and Commissioning of the Service**

Before the Operational Service Date and, where applicable, throughout the provision of the BTnet Security Service, the Customer will:

10.1.1 ensure that the LAN protocols and applications the Customer uses are compatible with the BTnet Security Service;

10.1.2 be responsible for security configuration, and for reviewing and requesting any changes to that configuration;

10.1.3 manage, and provide BT with accurate details of the internal IP address design;

10.1.4 obtain and provide in-life support for any software running on Users' devices; the security and operation of Users' devices is the Customer's responsibility; and

10.1.5 ensure that the Customer's network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request.

10.2 **During Operation**

On and from the Operational Service Date, the Customer will:

10.2.1 notify BT of any planned work that may cause an Incident;

10.2.2 permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove faulty BT Equipment in its entirety and exchange it with a functioning replacement. BT will use reasonable endeavours to ensure any data on recovered BT Equipment is rendered unreadable prior to disposal or recycling;

10.2.3 agree that the processing of customer information and Customer Personal Data will be subject to the relevant supplier's privacy policy as may be amended or supplemented from time to time by the supplier. The Customer agrees that BT will not be liable for any claim arising out of or in connection with any failure by the supplier to comply with the supplier's privacy policy and the Customer will make any claims directly against the supplier;

10.2.4 agree that the BTnet Security Service will operate in combination with the Customer's content or applications or with any other software, hardware, systems or data;

10.2.5 own all right, title and interest in and to all of the customer information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any customer information; and

10.2.6 be responsible for results that the Customer has obtained from the use of the BTnet Security Service, and for conclusions drawn from such use. BT will have no liability for any damage caused by errors or omissions in any information, instructions or scripts that the Customer has provided to BT in connection with the BTnet Security Service, or any actions that BT has taken at the Customer's direction.

10.3 **The End of the Service**

On notification of termination of the BTnet Security Service by either one of us, or notification of expiry of the BTnet Security Service, the Customer will be responsible for securing its Internet connection and will be liable for the increased risk it exposes itself to.

11 Service Levels

11.1 BT will provide the BTnet Security Service to the Customer on an "**as is**" and "**as available**" basis. BT does not guarantee that the BTnet Security Service will be performed error-free or uninterrupted or that BT will correct all errors in the BTnet Security Service.

11.2 The Customer acknowledges that neither the Service Levels in Part C (Service Levels) of the BTnet Service Schedule nor the Business Premium Care Level as further set out in the Support Services Schedule apply to the BTnet Security Service.

Part C – Defined Terms

12 Defined Terms

In addition to the defined terms in the Schedule, capitalised terms in this Annex will have the following meanings (and in the case of conflict between these defined terms and the defined terms in the Schedule, these defined terms will take precedence for the purposes of this Annex):

"**Blocked Categories List**" has the meaning given to it in Paragraph 3.3.1.

"**BTnet Security Service**" has the meaning given in Paragraph 1.

"**BTnet Security Operational Service Date**" means, for each BTnet Security Service, the date on which that BTnet Security Service is first made available to the Customer.

"**CIPA**" means the Children's Internet Protection Act.

"**Cisco AMP**" means the Advanced Malware Protection system provided by Cisco, or similar technology from time to time, used as part of the BTnet Security Service.

"**Content Filtering**" means web or URL filtering and does not include any email or file scanning.

"**Content Filtering System**" means a system that provides Content Filtering lists and databases, or similar technology from time to time, used as part of the BTnet Security Service.

"**CVSS**" or "**Common Vulnerability Scoring System**" provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

"**DNS**" means Domain Name System.

"**EULA**" has the meaning given in Paragraph 7.1.
"**HTTP**" means hypertext transfer protocol.
"**Intrusion Detection and Prevention System**" means an open source network intrusion prevention system and network intrusion detection system, or similar technology from time to time, used as part of the BTnet Security Service.
"**IWF**" means Internet Watch Foundation.
"**Layer 3 Firewall**" has the meaning given in Paragraph 3.1.
"**Layer 7 Firewall**" has the meaning given in Paragraph 3.2.
"**URL**" means Uniform Resource Locator (a website link).
"**VPN**" means Virtual Private Network.