Service Annex to the General Service Schedule
BT Managed Cloud Security (ScanSafe)

1 DEFINITIONS

The following definitions apply, in addition to those in the General Terms and Conditions and the General Services Schedule of the Agreement.

"**Administrator**" means a Customer authorised person responsible for managing the Service via the Customer Portal as described in Clause 2.7 below.
"**Change Order**" means the form to be used by the Parties to institute a change to the Services.
"**Customer Information**" means any Customer, product, support or other data or information provided by the Customer to BT in the course of BT providing the Service.
"**Customer Systems**" means the Customer's information and IT assets and systems that may be made available to BT from time to time to facilitate the performance of the Service.
"**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.
"**Internet**" means the global data network comprising interconnected networks using the TCP/IP protocol suite.
"**Professional Services**" means the professional services as set out in Clause 3.4 of this Service Annex.
"**Service**" means any combination of the component service options that are ordered by the Customer.
"**Service Deliverables**" means any and all things to be delivered by or on behalf of BT to the Customer, as more specifically described in an Order.
"**Service Operational Personal Data**" means all Customer Personal Data provided by the Customer under or in accordance with the Agreement that is operationally required for BT to contact the Customer for the provision of the Service such as email addresses, invoicing information, contact names, site addresses, telephone and fax numbers.
"**Web Content**" means the textual, visual or aural content that is encountered as part of the user experience on websites. It may include amongst other things: text, images, sounds, videos and animations.
"**Web Traffic**" means the data sent and received by visitors to a web site.

2 2 SERVICE OVERVIEW

BT Managed Cloud Security (ScanSafe), is based on the Cisco ScanSafe Web Security service. It enables the Customer to protect Users from Internet-borne web threats. The Customer can order some or all of the following options:

2.1 Malware Scanning (MS)

2.1.1 The Customer's unencrypted web pages and attachments will be scanned by Outbreak Intelligence TM, a proprietary security platform that detects malware threats by using a combination of multiple, correlated detection technologies, including anti-malware engines.

2.1.2 MS will scan as much of the web page and its attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Attachments that cannot be scanned will be blocked.

2.1.3 If the Customer's Web page or attachments contain malware (or cannot be scanned) in accordance with paragraph 2.1.2 (except for Secure Socket Layer (SSL) traffic), then access to that web page or attachment will be denied and an automatic alert web page will be displayed to the User. Notification will also be sent by email to the Customer Administrator (if that option has been chosen).

2.1.4 HTTPS Inspection is an additional option that allows the Customer Administrator to configure a policy specifying the domains and categories of HTTPS traffic to be decrypted and inspected by MS. User data is encrypted between the web browser and the scanning tower, and between the scanning tower and the Web server. However, for requests matching the HTTPS inspection policy, the scanning tower will terminate both sides of the SSL-based connection.

2.1.5 HTTPS Inspection can be used for both malware detection and enhanced web filtering actions such as Outbound Content Control (see 2.2.6 below). There are two options to enable HTTPS Inspection to operate without certificate warnings at the browser:

(a) A certificate is generated by the administration portal which must be installed on all Users' browser clients; or

(b) A certificate signing request (CSR) is generated by the administration portal. The organisation's Certification Authority (CA) is used to sign this, and then the resulting certificate is uploaded via the portal. In this case no additional Customer side deployment is required where the CA is already installed at the browser.

2.2 **Web Filtering (WF)**

2.2.1 Web pages and attachments will be filtered using URL categorisation and content analysis.

2.2.2 The Customer can configure WF to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, 'blocked' and 'allowed' list functionality) are also available.

2.2.3 WF will filter as much of the web page and its attachments as possible. It may not be possible to filter certain web pages or attachments (for example, password protected). The Customer may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (that is HTTPS/SSL) cannot be filtered and will be passed through WF unless otherwise specified by the Customer in relation to specific categories of content.

2.2.4 The Customer has the option of performing individual and/or group administration and reporting capabilities by using the Connector software described below.

2.2.5 If a User requests a web page or attachment where an access restriction policy applies, then access to that web page or attachment will be denied and an automatic alert Web page will be displayed to the User. Notification may also be sent by email to the Customer Administrator.

2.2.6 Outbound Content Control gives the Customer flexibility to define rules based on the HTTP protocol's POST function. These filters look for specific files with certain characteristics (e.g. M05 or SHA1 checksums), keyword analysis, outbound file types, or preconfigured recognisable information (e.g. credit card numbers or social security numbers).

2.3 **Secure Mobility**

2.3.1 Optional software (AnyConnect) is available. If the Customer orders it, it can download the AnyConnect software to install on its Users' PC or laptop devices, in accordance with installation guidelines.

2.3.2 AnyConnect allows the User's PC or laptop to connect to the Service from a remote location outside the Customer's internal network. AnyConnect allows integration of the Service with a wide range of Cisco appliances such as routers.

2.3.3 AnyConnect may not support all User device setups.

2.4 **Data Retention (DR)**

The standard Service will retain allowed traffic data for 45 (forty five) days and blocked traffic data for one year. If the Customer requires it, extended DR up to six months (or more if allowed under the applicable law) can be ordered at an additional Charge that will be stated on the Order.

2.5 **Passive Identity Management (PIM)**

2.5.1 PIM enables the Customer to deploy the Service with User level granularity without the need to install proxies onsite. PIM does this by embedding some encrypted information in the user agent string (a characteristic identification string) that the web browser passes to the Service. PIM is typically deployed as part of a login script. Traffic is directed as per standard deployments without a Connector; eg through the use of a PAC (proxy auto configuration) file.

2.5.2 PIM may not support all browser applications. Microsoft Active Directory group information is not passed within the login script.

2.6 **Customer Portal (Portal)**

2.6.1 BT will provide the Customer with log-in details required to allow the Customer to access to a Web-based portal, to administer and report on the Service. Access to the Portal is via a secure (https) website and is password-protected.

2.6.2 The Customer may allow multiple Administrators to access the Portal. The Customer is required to give each Customer Administrator a unique login and provide full access or read only privileges specific to each. This functionality allows a unique, single super User account that can create multiple Administrators.

2.6.3 The Portal enables the Customer Administrator to:

(a) review statistics of all malware stopped and other Web Content blocked;
(b) create access restrictions and apply these to specific Users or groups (if it has installed the Connector);
(c) customise browser alert pages seen by Users when web-access to a particular site or file is denied;
(d) update administration details for real-time email alerts; and
(e) configure and schedule automated system auditing and reporting.

2.6.4 Automated reports are available on overall traffic, bandwidth, blocked URLs and Web malware stopped. The Portal also offers a comprehensive selection of additional reports, generated daily, which provide in-depth analysis in the form of graphs, tables, and exportable data files. The Customer can schedule regular reports for different service functionality and specify Users, times, and email it to certain Users or groups.

2.6.5 Audit Logging functionality records administration, configuration, filtering, and policy changes made for the Service, and can be configured by the Customer Administrator or the Customer super User. Auditing includes what was changed, by whom and when. Audit logs can be searched by specifying a time period, category or type of logs, and type of action taken.

2.6.6 Privacy Logging functionality, when enabled, will log when web pages are blocked according to web filtering policy, but will obfuscate private details such as source username and IP address. This feature helps the Customer to comply with local privacy policies or regulations, where applicable.

2.6.7 Block Alert Pages are dynamically generated HTML pages displayed to Users when they are prevented from accessing prohibited Web Content. The Customer can choose a standard block alert page or its own customised content which can be uploaded via the Portal. A user guide is available to the Customer.

2.7 **Advanced Malware Protection (AMP)**

Advanced Malware Protection (AMP) is included in the Web Security Premium Bundle, and may be ordered separately by customers of the existing service. If ordered, ScanSafe will provide AMP technology to the Customer for performing file analysis at the gateway to detect malware threats. This functionality augments the anti-malware detection and blocking capabilities offered by Web Malware Scanning.

Cryptographic hashes of files are collected and transmitted to a ScanSafe-managed cloud service where analysis is performed and a disposition is made whether the file is malicious, neutral or unknown.

If a disposition is unable to be made after the analysis of the hash of a file, the Customer has the additional ability to submit the file to a separate cloud-based sandbox managed by ScanSafe for further analysis. The Customer can configure AMP to limit the type of files sent to the sandbox. After the file analysis is completed, reputation reporting, file behavior reporting and retrospective verdict alerting are accessible from the ScanCenter portal.

2.8 **Cognitive Threat Analytics (CTA)**

Cognitive Threat Analytics (CTA) is included in the new Web Security Premium Bundle and may be ordered by customers, together with AMP, as an upgrade to their existing service. If ordered, CTA performs a behavioral analysis of the web logs generated by the service and identifies anomalous traffic that indicates possible malware infections, malicious activity, or policy violations on the Customer network ("**Incidents**"). CTA generates Incident reports for the Customer which are accessible from the ScanCenter portal. The CTA Incident report lists Incidents that indicate possibly infected hosts on the Customer network that communicate through the service. The Customer is responsible for investigating and/or mitigating Incidents reported by CTA, and ScanScafe is not responsible for any investigation and/or mitigation of incidents.

3 SERVICE DELIVERY

3.1 BT shall use its reasonable endeavours to provide the Service within 10 (ten) Business Days from the date that a correctly completed Order and all technical information reasonably required by BT has been received from the Customer.

3.2 BT will notify the Customer that the Service has been enabled, and provide activation support to the Customer. BT will send to the Customer a welcome letter that will explain the necessary configuration changes required to be made by the Customer in order to use the Service. The Operational Service Date occurs once BT notifies the Customer that the Service has been enabled.

3.3 A Cisco Service Delivery Manager (SDM) is assigned to each new Order and provides implementation assistance to the Customer for the ScanSafe configuration. The Cisco SDM will provide guidance related to connector configuration, best practice for initial web filtering policy creation, setting up user granularity, ScanCenter portal training, and instruction on reporting. Cisco SDM will also work with the Customer to configure their own ASA/ISR/WSA devices by providing a configuration template.

3.4 Where integration with other BT services or configuration of BT managed devices is required, professional services provided by BT personnel ("**Professional Services**"), will be provided by BT as set out in the Order. BT will review the Customer requirements and advise on suitability of hardware / software and overall solution approach. BT will configure any BT managed customer devices that are required for connection with the ScanSafe service. BT can also provide additional consultancy services where needed and agreed with the Customer including assistance with initial policy creation. All BT Professional Services will be charged on a per day fee basis.

3.5 BT shall use its reasonable endeavours to meet any estimates regarding any timescales or any results projected in connection with the Professional Services. Any such estimates are targets only and are dependent upon the accuracy and completeness of the information supplied to BT by the Customer and third parties, the degree of assistance given by the Customer and the manner in which any results of the Professional Services are used. Accordingly the Customer acknowledges and agrees that the Professional Services may not be completed within the expected timescales or achieve the projected results.

3.6 BT shall not be responsible for the way in which the Customer uses the Deliverables or any other output from the Professional Services.

3.7 The Customer agrees that Customer Equipment and Customer Systems will be provided to or made available to BT at no cost to BT where necessary for use in performance of the Professional Services, subject to any security or other procedures that accompany such Customer Equipment or Customer Systems.

4 PERSONNEL

4.1 BT shall perform the Professional Services using such personnel as it considers suitably qualified. BT shall be solely responsible for directing, controlling and supervising the work performed by BT. BT reserves the right at any time to vary personnel upon reasonable notice to meet business and personal needs of personnel.

4.2 BT personnel engaged in the performance of the Professional Services shall at all times remain under the direction and control of BT and the conditions of employment of BT shall continue to apply to such personnel.

4.3 Subject to the provisions of the General Terms and Conditions (Confidentiality) nothing in this Service Annex shall prevent BT from assigning BT personnel performing the Professional Services from providing similar services for third parties or in any way restricting BT's use of such personnel.

4.4 The Customer shall not employ or engage as an independent consultant or offer such employment or engagement to any of BT's employees who are involved in providing the Professional Services, without BT's prior written agreement during the term of this Service Annex and for twelve months after its termination. If the Customer breaches this condition then BT may, in its sole discretion, charge the Customer a fee equivalent to one hundred days' work by that person at his/her then current full daily fee rate. This shall not apply where the BT employee successfully applies for a generally advertised Customer position that is demonstrably not intended to circumvent this non-solicitation restriction.

5 SERVICE MANAGEMENT BOUNDARY (SMB)

BT's Cloud Security service boundary is the point where the Customer's traffic (inbound or outbound) is presented to the ScanSafe infrastructure. The Service excludes the Customer's Internet transport, and configuration.

6 THE CUSTOMER'S RESPONSIBILITIES

The Customer will:

6.1 be solely responsible for the provision, maintenance and payment for its access connection to the Internet or any equipment necessary to make such connection.

6.2 direct external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) 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 (eg to the corporate intranet) is not directed via the Service.

6.3 supply BT with all its technical data and any other information BT may reasonably request from time to time to allow BT to supply the Service.

6.4 inform BT 5 (five) days in advance and provide details of any changes to the Customer network that may impact the working of the Service. This is so that BT may arrange for any necessary changes to the Service configuration. If this information is not provided, or is provided less than 5 (five) days before a change, then BT shall not be liable for any incorrect operation of the Service.

6.5 inform BT within 5 (five) days if the number of Users increases by more than 5% from the number of Users set out on the Order, in which case BT reserves the right to increase the Charges. BT reserves the right to require a new Order, if the number of Users shown by Web Traffic logs exceeds the number of Users set out on the original Order.

7 ACCEPTABLE USE POLICY

The following conditions apply in addition to the Acceptable Use Policy in the General Services Schedule.

The Customer's Users must not under any circumstances whatsoever commit, or attempt to commit, directly or indirectly any action that may threaten the Service, whether deliberate, negligently or otherwise. This shall include but is not limited to:

(a) interfering with the use of the Service by other authorised Users; altering, tampering with or circumventing any aspect of the Service;
(b) attempting to crash a Service host or network; e.g. "**denial of service**" attacks, or "**flooding**" attacks against a Service host or network;
(c) reselling, passing-through, renting, leasing, timesharing or branding the Service or otherwise providing the Service to any party which is not contractually authorised by BT to receive the Services;
(d) testing or reverse-engineering the Service in order to find limitations, vulnerabilities or evade filtering capabilities;
(e) supplying proprietary information about the Service, including but not limited to screen shots, product documentation, demonstrations, service descriptions, announcements, or feature roadmaps to unauthorised third parties;
(f) any excessive use of the Service that generates unreasonably and unnecessarily high traffic loads
(g) the creation, transmission, storage, or publication of any kind of virus or corrupting program or corrupted data.
(h) (h) using the Services for any unlawful, invasive, infringing, defamatory or fraudulent purpose;
(i) (i) any attempt to circumvent the user authentication or security of a Services host or network;
(j) (j) any other action that may adversely affect the Services or their operation

BT shall have the right to suspend or terminate the Services and to take such action as may, at BT's sole discretion, be deemed necessary in the event of any attack upon the Services or network, or if the Customer's use of the Services represents an imminent threat to the network, or if so directed by a court or competent authority. Furthermore, BT may instigate civil and/or criminal proceedings as appropriate as against the perpetrators of such prohibited action.

8 CHARGES AND PAYMENT TERMS

8.1 The Charges for the Service will comprise some or all of the following components, depending on the options selected on the Order:

Pricing Element	One-time Charge	Recurring Charge	How Charges will be applied
Malware Scanning		Monthly per User	
Web Filtering		Monthly per User	
Malware Scanning and Web Filtering		Monthly per User	
Web Security Premium Bundle		Monthly per User	
Secure Mobility (AnyConnect)		Monthly per User	
Data Retention		Monthly per User	
Advanced Threat Detection		Monthly per User	Minimum 1000 users
Advanced Malware Protection		Monthly per User	
Guest W-Fi (bandwidth based)		Monthly per bandwidth	
Log Extraction		Monthly per User	

Pricing Element	One-time Charge	Recurring Charge	How Charges will be applied
Professional Services/Ad-Hoc Consultancy	Per Day		

8.2 If additional Charges are incurred by BT, and not otherwise incorporated into a Change Order, as a result of:

(a) any alteration or addition to the Professional Services as detailed in the Order;
(b) abortive visits to the Site arising from failure or delay by the Customer in providing access to the Site;
(c) delays due to the Customer's failure to provide Customer Information; and/or
(d) failure or delays by the Customer in attending or arranging meetings reasonably required by BT in order to perform the Professional Services,

then the Customer shall be liable to pay such additional Charges.

8.3 **Changes to Customer Requirements**

If either **(a)** the Customer wants to add Users to an existing Service, and/or **(b)** add Service options to the existing Service ("**Changes**"), then following is required before such Changes will be accepted:

(i) for requested Changes to be implemented more than 60 (sixty) days from the end of the Minimum Period of Service, and whereby the Customer does not want to extend the Minimum Period of Service, the Parties first need to agree on new applicable Charges by signature of a Change Order;
(ii) for requested Changes to be implemented less than 60 (sixty) days from the end of the Minimum Period of Service, the new applicable Charges and a new Minimum Period of Service for the whole Service needs to be agreed by a Change Order.

Customer bandwidth-usage will be actively monitored and monthly usage reports will be generated. Customers exceeding monthly bandwidth usage beyond purchased limits for 2 consecutive months will be charged for additional bandwidth.

8.4 **Termination and Early Termination**

8.4.1 In variance to the General Terms and Conditions of the Agreement, either Party may terminate the Service by providing at least 30 (thirty) days' prior written notice to the other Party.

8.4.2 In variance to the General Service Schedule, if the Customer terminates the Service before the end of the Minimum Period of Service, then the Customer must pay, by way of compensation, all remaining Monthly Charges until the end of the Minimum Period of Service.

9 SERVICE LEVELS

The Service Levels as set out in the General Service Schedule apply to this Service, save for Availability which shall be replaced with 9.1 below.

9.1 **Service Availability**

The Service will process and deliver web requests 99.999% of the total hours during every month that the Customer uses the Service ("**Availability**"). Availability will be determined on an aggregate basis across all Customer sites. The Customer will be provided with both primary and secondary proxy addresses for each site from Web Traffic may be directed. As a result, non-Availability occurs only where Web Content sent from a site to both proxy addresses is not being received or transmitted to end users at the affected Customer site., The above applies only to downtime due in whole or in part to BT's inability to provide Service to the Customer which is not due to events of force majeure, or to acts or omissions by the Customer or its staff/officers/agents/contractors which are in contravention of this Agreement. The following Service Credits apply as sole and exclusive remedy for a breach of this Service Level.

Monthly Service Availability	Service Credit as percentage of Monthly Charges for the Service
99.999 - 99.5 %	10%
99.49 - 99.0 %	20%
98.99 - 98.5 %	30%
98.49 - 98.0 %	40%
97.99 - 97.5 %	50%
97.49 - 97.0 %	60%
96.99 - 96.5 %	70%
96.49 - 96.0 %	80%

Monthly Service Availability	Service Credit as percentage of Monthly Charges for the Service
95.99 - 95.5 %	90%
Less than 95.5%	100%

9.2 **Web Filtering Latency (WFL)**

WFL refers to the additional web page load time attributable to the web Services. WFL is assessed by reference to the average elapsed time between a web page request being sent to BT at the datacentre where the applicable scanning towers are located and receipt of the requested web-page data by the requesting party.

WFL shall be assessed solely by reference to the time taken to download a discrete resource from a selection of popular websites. For the avoidance of doubt the WFL SLA does not apply to the Anywhere+ service.

To calculate the average WFL, the average elapsed time taken to download a discrete resource will be measured from each of the websites referred to above ("**Filtered Response Time**") and compared to the average elapsed time taken for identical Web page requests by the same requesting party during the same testing period which are not processed through the Services ("**Unfiltered Response Time**"). Each such sample of the Filtered Response Time and Unfiltered Response Time is referred to as a "**Sampled Pair**". Such samples shall be taken every 60 minutes.

The Filtered Response Time (averaged over all of the Sampled Pairs) in any month will not exceed the greater of:

(a) one second more than the Unfiltered Response Time; and
(b) three times more than the Unfiltered Response Time.

If this measure is exceeded, a one-off Service Credit equal to 10% of the monthly Charges for the Service for that month will be applied.

9.3 **False-Positive Filtering Rate**

The "**False-Positive Filtering Rate**" Service Level measures the percentage of URLs and domains that were blocked by the Service but, based on the Customer's chosen categorization policies, should not have been blocked ("**Bad Blocks**"). For the avoidance of doubt, if a URL is in the 'unclassified' category it shall be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Positive Filtering Rate = 100% x total number of Bad Blocks in a Month at all Sites ÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same Month where the Bad Blocks are determined by BT acting reasonably.

BT shall respond within seven days of receipt of notification that the Customer believes there to have been a Bad Block, and BT shall give reasons for the decision as to whether there has been a Bad Block or not.

If the False-Positive Filtering Rate is greater than or equal to 0.0004%, a one-off Service Credit equal to 10% of the Monthly Charge for the Web Filtering Service will be applied.

9.4 **False-Negative Filtering Rate**

The False-Negative Filtering Rate Service Level measures the percentage of URLs and domains that were not blocked by the Service but, based on the Customer's categorization policies, should have been blocked ("**Missed Blocks**"). For the avoidance of doubt, if a URL is in the 'unclassified' category it shall only be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Negative Filtering Rate = 100 x total number of Missed Blocks in a Month at all Sites ÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same Month where the Missed Block are determined by BT acting reasonably.

BT shall respond within seven days of receipt of notification that the Customer believes there to have been a Missed Block, and BT shall give reasons for the decision as to whether there has been a Missed Block or not.

If the False-Negative Filtering Rate is greater than or equal to 0.0004%, a one-off Service Credit equal to 10% of the Monthly Charges for the Web Filtering Service will be applied.

9.5 **Service Credits**

9.5.1 Service credits do not apply to any matters arising due to any of the following:

9.5.1.1 Customer requested hardware or software upgrades, moves, facility upgrades etc.

9.5.1.2 a scheduled maintenance period that was announced at least 24 hours in advance.

9.5.1.3 hardware, software or other data centre equipment or services not in the control of BT or within the scope of the Service.

9.5.1.4 hardware or software configuration changes made by the Customer without the prior written consent of BT.

9.5.1.5 denial of Service attacks on the installed email security infrastructure or ancillary services.

9.5.2 Service credits are not cumulative. No more than one category of service credit, as described in Clauses 9.1, 9.2, 9.3 and 9.4, may be claimed in respect of any one event or issue.

9.5.3 For the avoidance of doubt, while BT will use its reasonable endeavours to detect malware, BT does not guarantee that the Services (including AMP and CTA) will detect or block any specific malicious threat.

10 SERVICE OPERATIONAL PERSONAL DATA

In order for BT to provide and support the Service, BT may use Service Operational Personal Data in order to:

(a) process, track and fulfil Orders for Service;
(b) deliver and commission the Service, either remotely or at the Site;
(c) process, track and resolve incidents with the Service, either remotely or at the Site;
(d) administer access to online portals relating to the Service;
(e) compile, dispatch and manage the payment of invoices relating to the Service;
(f) manage the contract and resolve any disputes relating to it; or
(g) respond to general queries relating to the Service.

BT may also use the Service Operational Personal Data to send additional information concerning the Service, or related services, to the Customer. If this information includes marketing materials, BT will provide a mechanism for the recipient to elect not to receive such communications in the future.

11 PERSONAL DATA

Any Customer personal data may be processed in accordance with the Cisco privacy policy, as may be amended from time to time, which is set out at: http://www.cisco.com/web/siteassets/legal/privacy_full.html.