BT Managed Firewall Security
Service Annex to the General 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 and the General Services Schedule of the Agreement.

"**Acceptance Tests**" means those objective tests conducted by the Customer, which, when passed confirm that the Customer accepts the BT Managed Firewall Security Service as free of material faults and that the BT Managed Firewall Security Service is ready for use save for any minor non-conformities, which will be resolved without undue delay after the Operational Service Date.
"**Active Active**" has the meaning give in Paragraph 2.2.10.
"**Active Passive**" has the meaning given in Paragraph 2.2.10.
"**BT Owned**" has the meaning given to in Paragraph 2.1.1.
"**BT Takeover**" has the meaning given in Paragraph 2.1.1.
"**Critical CVSS score**" means a CVSS score range from 9.0 to 10.0.
"**Customer Equipment**" means any equipment (including any purchased and owned by the Customer) and any software, other than BT Equipment, used by the Customer in connection with the Service.
"**Customer Portal**" means one or more webpages made available to the Customer by BT to provide for one or more specific functions in relation to the Service.
"**Customer Owned**" has the meaning given in Paragraph 2.1.1.
"**CSP**" means the Customer's Security Policy containing the security rules, set and owned by the Customer that are applied to the BT Equipment or Customer Equipment and determine the operation of the BT Managed Firewall Security Service.
"**CVSS**" means Common Vulnerability Scoring System v3.0.
"**DMZ**" means "**demilitarized zone**" (sometimes referred to as a perimeter network), a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**Emergency Change**" means a change that requires immediate attention from SOC to address a live, service impacting issue that the Customer is experiencing. Emergency Change should be used only as a last resort.
"**Enabling Service**" has the meaning given in Paragraph 4.1.2.
"**Ethernet**" means a family of computer networking technologies for LANs.
"**EULA**" has the meaning given in Paragraph 4.1.3.
"**Firewall Intrusion Detection and Prevention Service**" means the Service Option as set out in Paragraph 2.2.3.
"**High CVSS score**" means a CVSS score range from 7.0 to 8.9.
"**IPSec**" means IP security; it is a standards-based framework that provides layer 3 services for confidentiality, privacy, data integrity, authentication and replay prevention.
"**Incident**" means a fault; an unplanned interruption to, or a reduction in the quality of, the Service or particular element of it.
"**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.
"**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.
"**Local Area Network**" or "**LAN**" means the infrastructure that enables the ability to transfer IP services within Sites (including data, voice and video conferencing services).
"**MPLS**" means Multi-Protocol Label Switching, a private, global IP-based VPN service based on industry standards that provides the Customer with any-to-any connectivity and differentiated performance levels, prioritisation of delay and non-delay sensitive traffic as well as voice and multi-media applications, all on a single network.
"**Nominated Representative**" means a person from the Customer's organisation nominated to be the point of contact for Vulnerability notifications.
"**Out of Band Access**" means access used for initial configuration and for in-life management where the primary means of access to the Security Appliance has failed or to help resolve failure of the Security Appliance.
"**Patch**" means vendor provided Software intended to address a specific Vulnerability.
"**Professional Services**" means those services provided by BT which are labour related services.
"**PSTN**" means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.
"**Resilient Component**" means, with respect to a Resilient Service, any of the access lines, BT Equipment or Customer Equipment.

"**Resilient Service**" means a Service or part of a Service, as set out in the Order that is designed to have high availability and without single points of failure, such that if one component fails the Service is still available.
"**Router**" means a device that forwards data packets between computer networks, creating an overlay internetwork.
"**Security Appliance**" means the BT Equipment or Customer Equipment (depending on the Service delivery model the Customer selects in accordance with Paragraph 2.1.1) used to apply the CSP.
"**Service Desk**" means the BT helpdesk for reporting any Incidents and inquiries about the Service.
"**Service Management Fee**" means the fee that will cover inlife management and simple changes submitted via BT's change management system subject to reasonable use criteria set out in Paragraph 2.1.5.6.
"**Service Management Boundary**" has the meaning given in Paragraph 3.5.1.
"**Service Options**" has the meaning given in Paragraph 2.2.
"**Service Wrap Only**" has the meaning given in Paragraph 2.1.1.
"**Site Planning Guide**" means a guide provided by BT to the Customer detailing the hardware specification, including environmental, physical and electrical details of any BT Equipment provided to the Customer with the BT Managed Firewall Security Service.
"**SOC**" means Security Operations Centre.
"**Standard Change**" means upgrades and modifications resulting from planned developments and security improvements.
"**Standard Service Components**" has the meaning given in Paragraph 2.1.
"**Threat Emulation Service**" means the Service Option as set out in Paragraph 2.2.7.
"**Uniform Resource Locator**" or "**URL**" means a character string that points to a resource on an intranet or the Internet.
"**Urgent Change**" means 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.
"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to the Customer's Users while being provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, the Customer's communications over the Customer's VPN are restricted to those Sites belonging to the Customer's VPN.
"**Vulnerability**" means a Software susceptibility that may be exploitable by an attacker.
"**Wide Area Network**" or "**WAN**" means the infrastructure that enables the transmission of data between Sites.

2 Service Description

BT Managed Firewall Security ("**Service**") provides the Customer with a managed firewall Service located at a Customer Site or hosted at a BT Site.

The Service controls inbound and outbound access to the Internet, performing functions that may include control of inbound traffic according to controlled exceptions (firewall), managing Users' outbound web access according to pre-defined policy (URL filtering), and scanning traffic to block malware (anti-virus). The Service is made up of various "layers", described in Paragraph 2.1 with options according to Customer requirements.

The Service and/or some of the Service components may not be available in all locations. In such circumstances the Parties may agree in writing that the Customer will arrange – either in its own name or via a third party – the provision of the Service elements at locations where BT is unable to supply them and the applicable conditions for doing so.

2.1 Standard Service Components

The following standard Service elements are provided by BT.

2.1.1 **Security Appliance**. The Customer may choose from a range of security appliances. Alternatively, BT will recommend an appliance (or appliances) as part of the overall service design. The Customer may request to use Customer Equipment for the Service. BT's agreement to such a request is subject to an assessment by BT that the Customer Equipment is suitable for use with the Service and BT's written confirmation that BT can support the Customer Equipment.

The Customer will select one of the following delivery models. The table below sets out the responsibilities of the Parties for the supply and management of Security Appliances, other Equipment, installation, commissioning, support agreements (incl. software and licences), remote service management and on-site support, unless otherwise specified in the Order:

Description	BT Owned	Customer Owned	BT Takeover	Service Wrap Only
Security Appliance	BT (new)	Customer (new)	Customer (pre-existing)	Customer (new)
Other equipment (including BT Equipment), including Out of Band Access and switches	BT (new)	BT (new)	BT (new) or Customer (pre-existing) as specified	Customer (new)
Installation	BT	BT	Customer (pre-existing)	Customer
Commissioning	BT	BT	Customer (pre-existing)	BT
Support agreements, software and licensing	BT	BT	BT	Customer
Remote service management	BT	BT	BT	BT
On-Site support	BT	BT	Customer's supplier; but BT will raise the necessary support requests on Customer's behalf for any failure in Customer Equipment that BT detects	Customer's supplier; but BT inform the Customer of any failure in Customer Equipment that BT detects

2.1.2 **Security Applications**. An appropriate security application licence (e.g. for firewall or URL filtering software) will be provided by BT as part of the Service.

2.1.3 **Project Managed Installation**. A BT project manager will coordinate the Service installation and its commissioning, liaising with the Customer, installers, equipment suppliers and network suppliers, as appropriate (e.g. according to whether BT Equipment or Customer Equipment is being used). All project management activity will be administered remotely and the named representative will not visit the Customer's Site.

2.1.4 **Incident Management**. This provides a 24x7 Service Desk to respond to faults, on-site equipment maintenance backed off to appliance and application vendors, and continuous real-time Service monitoring.

2.1.5 **Changes to the CSP**.

2.1.5.1 Where the Customer requires a change to the CSP, for example as a result of changes to the Customer's application requirements or network environment, the Customer may request additions, deletions, or modifications to the CSP and BT will provide the Customer with the means to request Standard Changes or Urgent Changes to the CSP, either on the relevant Customer Portal or to the Service Desk.

2.1.5.2 The CSP changes described in this Paragraph refer only to requests to change the rule-sets that define the BT Managed Firewall Security Service's operation. BT will only make configuration changes as set out in this Paragraph.

2.1.5.3 Following implementation targets apply for Standard and Urgent Changes and the completion time for the change will be notified to the Customer by BT.

Request	Implementation Target
Urgent Change and Emergency Change	4 Hours
Standard Change	8 Hours

Note: These implementation targets will not apply if the Customer submits a change with more than five (5) lines of changes.

2.1.5.4 BT will use reasonable endeavours to identify errors or potential unforeseen consequences of the Customer's requested CSP changes and advise the Customer appropriately and will not be liable for any consequence arising from:

(a) the Customer's misspecification of the Customer's security requirements in the CSP; or
(b) unforeseen consequences of a correctly specified and correctly implemented CSP.

2.1.5.5 The Customer will order separately any changes to the Service that are required and that involve physical changes to the Service, including Security Appliance upgrades and LAN re-arrangements. For

changes that require additional hardware, licences or changes to Charges (including changes to ongoing Recurring Charges) or where the solution needs to be re-defined, BT:

(a) will offer the Customer Professional Services in accordance with Paragraph 2.2.112.2.11; or

(b) agree a change to the Agreement that will only be effective if in writing and signed by both Parties.

2.1.5.6 BT will apply the following "**reasonable use**" restrictions for changes to the CSP:

(a) the Customer will not raise Standard Change requests more frequently than:

(i) two (2) per month per small firewall

(ii) four (4) per month per medium firewall; or

(iii) eight (8) per month per large firewall.

The respective Order will set out if a firewall is small, medium or large.

(b) Where BT's measurements show that change requests are being raised more frequently than the "**reasonable use**" restrictions, BT may, either:

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

(ii) review the Customer's requirements and agree with the Customer an appropriate alternative implementation process and any associated charges; or

(iii) require extra Charges for any changes above the "reasonable use" restrictions. Such shall be agreed in writing.

(c) access to the BT Customer Portal is controlled and will not be shared by the Customer's employees. All User ID tokens/passwords are to be uniquely assigned to named individuals. These individuals will not:

(i) allow anyone else to use their token/ID or share passwords;

(ii) leave their User account logged in while the computer is unattended and unlocked;

(iii) submit any unauthorised changes; or

(iv) attempt to access data that they are not authorised to access.

2.1.5.7 Customer Contacts are required to report the loss of any tokens or compromised passwords within the Customer's own organisation as per the Customer's standard security processes and to BT immediately.

2.1.6 **Service Performance Reports.** BT will provide near real-time or historic reports for key Service performance metrics, and for security-related events. This may be either via a Customer Portal, or a reporting application provided by BT and installed on a server owned by the Customer which needs to be selected by the Customer on the Order.

2.2 **Optional Services**

Following options are available subject to additional Charges and conditions as set out in the Order:

2.2.1 **IPSec VPN.** BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards:

(a) Site to Site VPNs between two (2) Security Appliances which are both owned by the Customer and managed by BT;

(b) remote access VPNs, for remote Users to gain secure access to the Customer's internal network. BT will implement the Customer's rules to authenticate against the Customer's authentication server. The Customer is responsible for providing and managing the Customer's own end-user VPN software; and

(c) third party (extranet) VPNs, for creating a site-to-site VPN between the Customer's Security Appliance managed by BT, and a Security Appliance owned or manged by the Customer or a third party. BT will only deliver VPNs to Security Appliances managed by a third party after the Operational Service Date.

2.2.2 **De Militarized Zones (DMZs).** BT will provide additional LAN segment interfaces on the Security Appliance, or on an adjacent network switch, according to the Customer's requirements. This is subject to there being sufficient physical ports available and additional Charges will apply if additional hardware is required to provide the interface.

2.2.3 **Firewall Intrusion Detection and Prevention Service:**

(a) BT will:

(i) monitor traffic passing through the Customer's Security Appliance for attacks, in accordance with the applicable intrusion signature files;

(ii) implement this Service Option with a default configuration setting, including a standard signature list. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the supplier but will not be responsible for evaluating these signatures beforehand;

(iii) where "**bronze level services**" are selected in the Order, block high impact or high confidence attacks, as defined by the supplier of the Software used to deliver the Firewall Intrusion Detection and Prevention Service. Bronze level services do not include monitoring, alerting or Service specific reporting and it will not be possible to make changes to this standard signature list. However, BT will disable the appropriate signature (or signature group if necessary) if the Customer advises BT of a conflict with any of the Customer's legitimate business traffic; and

(iv) where "**platinum level services**" are selected in the Order, apply additional signatures in "**detect**" mode. BT will provide 24x7x365 monitoring alerts relating to suspected intrusion incidents and categorise the alarm according to its severity. In the event that a high priority threat is discovered, BT will use reasonable endeavours to notify the Customer as soon as practical and ask the Customer if the Customer wishes to block the traffic causing the alert. BT will not proactively initiate this block in the absence of the Customer's instructions. BT will provide incident reports as part of this Service Option via the relevant Customer Portal.

(b) If BT agrees a request from the Customer to alter the parameters for applying new signatures in "**block**" mode, to give a greater or lower sensitivity to attacks, the Customer accepts responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

2.2.4 **Firewall URL Filtering and Application Control:**

(a) BT will:

(i) block access to those URLs that the Customer asks BT to, in accordance with the CSP. Internet sites are arranged into groups which are regularly updated. The Customer may choose to block or restrict access to any or all groups;

(ii) send an appropriate message to a User attempting to access a blocked or restricted site to advise either:

i. that the User request has been blocked; or

ii. that the User will first confirm acceptance of the Customer's acceptable use policy (or similar warning). Upon acceptance, the page will be delivered; and

(iii) implement the necessary alterations via the standard configuration management process in the event of any change in the CSP.

(b) This Service Option does not include reporting as standard. Reporting is available if the Customer has ordered the option Security Event Reporting as set out in Paragraph 2.2.8.

2.2.5 **Firewall Anti-Virus:**

(a) BT will:

(i) check web browser (http) traffic for known malware;

(ii) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and

(iii) keep antivirus definition files up to date by regular downloads direct from the antivirus Service.

(b) Provision of this Service Option is subject to a maximum file size and compressed archive limits, depending on the Security Appliance selected.

(c) This Service Option does not include reporting as standard. Reporting is available if the Customer has ordered the option Security Event Reporting as set out in Paragraph 2.2.8.

2.2.6 **Firewall Anti-Bot Service:**

(a) BT will check and block outbound traffic for communication with known "**command and control**" servers used by owners of malicious software.

(b) This Service Option does not include reporting as standard. Reporting may be available as an option depending on the Security Appliance being used.

2.2.7 **Threat Emulation Service:**

(a) BT will encrypt suspected malicious files and send them to the vendor's cloud-based infrastructure where they will be decrypted and analysed for malware by reviewing its behaviour in a virtual environment (sandbox).

(b) Depending on the Security Appliance the Customer selects, the Customer may be able to choose whether to hold the file whilst it is being analysed (to provide increased security) or to release it and analyse it in the background (for improved User response). Background processing may lead to malicious files being permitted until signature updates are subsequently generated and applied to the Customer's Security Appliances.

(c) If a file is deemed malicious, its characteristics will be added to the vendor's anti-virus signature list.

(d) BT will determine the country in which this inspection and analysis occurs.

(e) If the Customer requires the Service to protect against malware contained within SMTP (email) attachments, the Customer will arrange for the Customer's DNS mail exchange records to be re-directed to the Security Appliance so that email is delivered to that Security Appliance. BT will configure the Security Appliance to deliver email to the Customer's email server.

(f) Submission and processing of the Customer's data via the Threat Emulation Service will be at the Customer's sole discretion and at the Customer's own risk. Other than BT's obligations as set out in the General Terms and Conditions, BT assumes no responsibility or liability for the receipt and processing of such data.

2.2.8 **Security Event Reporting:**

(a) BT will provide reporting facilities, either on-line or on a server hosted on the Customer's Site, which allows analysis of security-related events but will not pro-actively view the Customer's reports and events for security incidents.

(b) If this Service Option is delivered via a shared reporting platform, BT will configure the platform such that the Customer is only provided with access to the Customer's reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform.

(c) The period over which data can be analysed is dependent on the capacity of the Security Appliances or the space allocated on the reporting platform.

2.2.9 **Identity Awareness / User groups:**

(a) BT will configure the features of the Security Appliance that support the Identity Awareness/User groups Service Option to apply certain rules of the CSP according to the authenticated identity of the User rather than just their IP Address.

(b) This may require client Software to be installed within the Customer's network or on end-user devices, or ensuring BT has remote, read-only, access to the Customer's active directory authentication server.

(c) The Customer will maintain the authentication database of Users, groups and any access credentials that the Customer requires.

2.2.10 **High Availability (dual appliance) solutions:**

(a) BT will configure a pair of Security Appliances on a single Site to give increased resilience against failure.

(b) Each Security Appliance may be connected to a separate Internet circuit to provide further resilience as set out in the Order.

(c) This Service Option will require additional switches to be included as part of the solution which will be provided by BT or the Customer as set out in Paragraph 2.1.1. If it is the Customer's responsibility to provide the additional switches, BT will advise the Customer of the number and type of switches required.

(d) Depending on the Security Appliances used and the CSP, BT may configure the Security Appliances as "**Active Active**" (both Security Appliances share the load under normal conditions) or "**Active Passive**" (one Security Appliance handles the load under normal conditions, with failover to a secondary Security Appliance in the event of the primary Security Appliance failing).

(e) For "**Active Active**" configurations, throughput performance may reduce under failure conditions unless each Security Appliance has capacity to handle the full load independently.

2.2.11 **Ad Hoc technical support / Professional Service:**

(a) BT will provide ad hoc technical support, chargeable per day, as set out in the applicable Order.

(b) Professional Services are delivered remotely unless otherwise set out in the Order.

2.2.12 **CSP production.** CSPs can be complex to define, so BT consultancy is available to help capture Customer requirements. If the Customer orders this (chargeable) option,

(a) BT will provide Professional Services to assist the Customer in the production and implementation of the CSP for a period of three (3) Business Days whereby BT will capture the necessary information in consultation with the Customer contact, and will produce the necessary CSP.

(b) If additional time for the creation of the CSP is needed, it will be charged for as set out in Paragraph 5.

2.2.13 **Vulnerability Notification and Patching:**

(a) BT will identify, test and implement Patches for High and Critical CVSS scores in accordance with the Customer's authorisation;

(b) the Vulnerability Notification and Patching Service Option will only be available while the Security Appliance is supported by the vendor.

3 BT's Responsibilities

In addition to any other BT obligations as set out in the Agreement:

3.1 Prerequisites

Throughout the provision of the Service, BT will:

3.1.1 provide the Customer with contact details for the Service Desk;

3.1.2 comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Site(s) and that the Customer has notified to BT in writing as long as such compliancy by BT shall not cause BT being in breach of any of its obligations under this Agreement.

3.2 Service Delivery

Before the Operational Service Date and, where applicable, throughout the provision of the Service, BT will:

(a) provide the Customer with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date;

(b) where applicable, arrange for any surveys to be conducted to confirm the availability of a suitable environment for provision of the Service (including confirming the presence of Enabling Services);

(c) will install or arrange for the installation by third party suppliers on BT's behalf of the Security Appliances at a Site as follows:

(i) if the Customer selects the BT Owned delivery model, BT will provide, install and commission any BT Equipment, including any hardware and software, licensing and support agreements for the Security Appliance and will arrange for any on-Site support and remote service management; and

(ii) if the Customer selects the Customer Owned delivery model, BT will install and commission that Customer Equipment, including hardware and software, licensing and support agreements for the Security Appliance to BT's specification and will provide on-Site support and remote service management;

(d) will provide the Customer with the Site Planning Guide;

(e) will appoint a named representative to be the Customer's single point of contact for the delivery of the Service; and

(f) will seek to validate that the Customer has ordered the correct number of licenses to serve the Customer's requirements, in accordance with vendor commercial terms and according to information provided by the Customer. If the Customer has not ordered sufficient licences BT will notify the Customer and the Customer must seek to rectify the situation within 30 days of the date of notification. If the situation is not resolved within this time such shall be considered as a material breach in accordance with the General Terms and Conditions. In any event, Customer is liable for breaches of vendor commercial terms, where BT is acting on information provided by the Customer.

3.3 Commissioning of the Service

Before the Operational Service Date, BT will:

3.3.1 contact the Customer and agree installation date(s), including access for third party installers;

3.3.2 once the Security Appliances are installed, BT will configure the BT Service remotely in accordance with the CSP;

3.3.3 deploy and configure the Service Option(s) selected by the Customer;

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

3.3.5 on the date that BT has completed the activities in this Paragraph 3.3, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

The Operational Service Date occurs when BT has configured and commissioned the Service, unless the Customer delays commissioning for any reason, in which case the Operational Service Date occurs on the installation date of the appliances.

3.4 **During Operation**

On and from the Operational Service Date, BT:

3.3.6 will, for a period of five (5) Business Days after the Operational Service Date, implement any simple changes or corrections to the CSP that may be necessary for the operation of the Service. BT will implement such changes as soon as reasonably practicable and they will typically involve individual lines of port/protocol, routing or network address translation changes. Any substantial changes to the CSP will incur additional Charges as set out in Paragraph 5 and may be scheduled for implementation following this five (5) Business Day period;

3.3.7 will maintain any relevant Customer Portal and server to provide the Customer with online access to a range of functions including performance reports and placing CSP change requests in accordance with Paragraph **Error! Reference source not found.**;

3.3.8 may carry out Planned Maintenance from time to time and will use reasonable endeavours to inform the Customer at least five (5) Business Days before any Planned Maintenance on the Service. For the avoidance of doubt any Emergency Maintenance shall not be considered as Planned Maintenance. Emergency Maintenance may be performed without advance notice to the Customer;

3.3.9 will, in the event of a security breach affecting the Service, contact the Customer and may require the Customer to change any or all of the Customer`s passwords;

3.3.10 will, if the Customer selects either the BT Owned, Customer Owned or BT Takeover delivery model, manage the ongoing maintenance, monitoring and configuration of BT Equipment or Customer Equipment for the duration of the Service. In addition, unless specifically agreed otherwise, BT may install additional BT Equipment on the Customer's Site, for the purpose of monitoring and management of the BT Service;

3.3.11 will, if the Customer selects any of BT Owned, Customer Owned or BT Takeover delivery models, be responsible for ensuring software licences and any required support contracts are renewed for the term of this Agreement. Unless the Customer gives BT written notice of an intention to terminate the Service 90 days before the end of the software licence term, BT will extend the software licences and any required support contracts for a further twelve (12) months;

3.3.12 will use secure protocols or provide a secure management link to connect to the Security Appliance via the Internet or other agreed network connection, in order to monitor the Service proactively and to assist in Incident diagnosis;

3.3.13 will provide an Out of Band Access link that connects directly to the Security Appliance(s), via a modem provided by BT and a PSTN direct exchange line provided by the Customer to allow further remote management and diagnostics capability;

3.3.14 will, if the Customer selects the CSP production Service Option, capture the necessary information in consultation with the Customer Contact and produce the CSP;

3.3.15 will continuously monitor the Customer's Security Appliances at regular intervals over the Internet or other agreed network connection;

3.3.16 will respond and remedy any Incident reported by the Customer as set out in the General Service Schedule. For any of the BT Owned, Customer Owned and BT Takeover delivery models BT provides 24x7x365 on-Site maintenance response where this is available locally. Where this level of cover is not available, on-Site support will be provided between 08:00 hours to 17:00 hours Monday to Friday excluding local public holidays in the relevant country;

3.3.17 will send the Customer a report securely via email if Vulnerabilities reported as having a CVSS score of 7.0 or above are identified. In the report, BT will advise the Customer's Contact of potential High and Critical CVSS scores. BT will not assess the configuration of a Security Appliance (a security policy or internal settings) or contextual exposure of any Security Appliances to the Vulnerability;

3.3.18 will use reasonable efforts to obtain a Patch for the Vulnerability from the Security Appliance vendor and will then test the Patch for installation and BT`s ability to roll-back the Software to the level prior to installing the Patch. Once testing is complete, BT will advise the Customer that the Patch is available for installation and provide additional information, where available, to support the Customer in deciding whether to install the Patch or not;

3.3.19 will, following the Customer's request to implement the Patch, agree an installation window with the Customer and confirm to the Customer when the Patch has been installed; and

3.3.20 will roll the Patch back upon the Customer's request in the event that the Customer detects undesirable side-effects. Any activity by BT required to resolve issues resulting from the implementation of a Patch is not covered by the Vulnerability Notification and Patching Service Option and BT will invoice the Customer additionally.

3.4 The End of the Service

On termination of the Service by either Party, BT will:

3.4.1 terminate any rights of access to the relevant Customer Portal and relevant Software and stop providing all other elements of the Service;

3.4.2 disconnect and remove any BT Equipment located at the Sites;

3.4.3 delete any Content; and

3.4.4 where requested by the Customer, provide, where reasonably practical, configuration information relating to the Service provided at the Site(s) in a format that BT specifies, provided the Customer has, at that time, paid all Charges outstanding at and resulting from termination (whether or not due at the date of termination) and signed prior to the termination an Order for such information and its applicable additional Charges.

3.5 Service Management Boundary (SMB)

3.5.1 BT will provide and manage the Service as set out in this Annex and as set out in the Order up to:

(a) the Internet/WAN side: the cable connecting the firewall to the Customer's Router;
(b) the LAN side: the Ethernet port(s) on the firewall or the switch provided by BT; and/or
(c) the analogue exchange line: the cable connecting BT's provided modem to the PSTN socket,

3.5.2 BT will have no responsibility for the Service outside the Service Management Boundary, including:

(a) issues on Users' machines or the Customer's servers (e.g. operating system, coding languages and security settings);
(b) end to end network connectivity (e.g. the Customer's network or Internet connectivity); or
(c) identity source management.

3.5.3 BT does not make any representations, whether express or implied, about whether the Service will operate in combination with any Customer Equipment or other equipment and software.

3.5.4 BT is not responsible if BT is unable to deliver the Service because of a lack of capacity on the Customer's selected Security Appliances.

3.5.5 BT cannot guarantee a) that the Service will operate without Incident or interruption or to intercept or disarm all malware and b) the security of the Service against unauthorised or unlawful access or use.

3.5.6 BT will provide the Service to the Customer on an "as is" and "as available" basis. BT does not guarantee that the Service:

(a) will be performed error-free or uninterrupted or that BT will correct all errors in Service;
(b) will operate in combination with the Customer's content or applications or with any other software, hardware, systems or data;
(c) including any products, information or other material the Customer obtains under or in connection with this Agreement, will meet the Customer's requirements; and
(d) will detect or block all malicious threats;

3.5.7 BT 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;

3.5.8 The Customer will own all right, title and interest in and to all of the Customer's information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any of the Customer's information; and

3.5.9 The Customer will be responsible for results obtained from the use of the 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 provided to BT by the Customer in connection with the Service, or any actions taken by BT at the Customer's direction.

4 The Customer's Responsibilities

4.1 Prerequisites

4.1.1 **Employer Disclosure.** As this Service enables BT to monitor and report to the Customer the use of any targeted applications, the Customer will comply with the employer disclosure obligations as set out in the General Service Schedule.

4.1.2 **Enabling Service**

4.1.2.1 The Customer will have the following Enabling Services in place that are necessary for the Service to function and will ensure that these Enabling Services meet the requirements provided by BT at contracting:

(a) Internet connectivity;
(b) WAN connectivity;
(c) PSTN direct exchange line, to enable Out of Band Access management;
(d) LAN/DMZ connectivity and associated infrastructure;
(e) PSTN connectivity; and
(f) broader IT environment, including the Security Appliances where they are the Customer's responsibility, including authentication services, additional switches where required, server/client platforms, security incident and event management (SIEM) solutions,

4.1.2.2 If BT provides the Customer with any services other than the Service (including, but not limited to any Enabling Service), this Annex will not apply to those services and those services will be governed by their separate terms.

4.1.3 **End User Licence Agreement (EULA)**

4.1.3.1 Depending on the respective vendor technology selected by the Customer for this Service; it may be required for the Customer to accept additional supplier end-user (license) agreement(s) ("EULA"). In such event BT will only provide the Service if the Customer has entered into the EULA(s) with the supplier in the form set out in the respective Order.

4.1.3.2 As the EULA may be amended or updated from time to time, the Customer hereby acknowledges having read and accepted the latest version of the respective EULA provided by BT before placing an Order with BT for the Service.

4.1.3.3 The Customer will enter into the EULA(s) for the Customer`s own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA(s) 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 the Customer or the supplier as such loss or damage will not be enforceable against BT.

4.1.3.4 The Customer will observe and comply with the EULA for any use of the applicable Software. If the Customer does not comply with the EULA:

(a) BT may restrict or suspend the Service upon reasonable notice,:
(b) the Customer will continue to pay the Charges for the Service until the end of the Minimum period of Service; and
(c) BT may charge a re-installation fee to re-start the Service.

4.1.3.5 Where the EULA(s) 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(s). For this purpose, the Customer hereby already grants to BT a mandate to enter into the EULA(s) in the Customer's name and on its behalf. BT and the Customer may for this also execute a power of attorney as part of the Order.

4.1.4 **Import and Export**

4.1.4.1 The Service includes components subject to export control as set out in the General Terms and Conditions. This applies specifically for countries where the use and import of encryption software and devices might be restricted by local law and regulations or the export and re-export of the encryption software or devices might be subject to the United States of America export control law. Non-observance of these export control conditions shall be considered as a material breach in accordance with the General Terms and Conditions.

4.1.4.2 If it is agreed to provide all or part of the Service using BT Equipment, BT will provide the Service with due regard for local country laws. This includes obtaining (if required) local import and export licenses and the written authority from all respective authorities. In countries where user licenses apply; the Customer agrees that it is responsible for, and will ensure that it complies with, all applicable licensing and regulatory requirements for use of the Service including but not limited to the local law and regulations that apply to the export and re-export of any encryption software or devices. BT reserves the right to require the Customer to produce proof of compliance with such licensing and regulatory requirements before Service delivery. If the Customer cannot produce such proof, BT reserves the right to suspend Service delivery or cancel the Order. If BT cancels the Order the provisions regarding cancellation as set

out in the General Terms and Conditions shall apply. The Customer is responsible for obtaining any local user licenses and the written authority from all respective authorities necessary.

4.1.4.3 If it is agreed to provide all or part of the Service using Customer Equipment whereby the Customer has arranged connection either on its own or via a third party from locations where BT cannot provide Service, the Customer is responsible for ensuring compliance with any applicable laws and regulations, including obtaining (if required) local import, export and user licenses and the written authority from all respective authorities free of charge for BT.

4.2 **Service Delivery**

Before the Operational Service Date and, where applicable, throughout the provision of the Service; the Customer will be responsible for the following:

4.2.1 **Information**. The Customer will provide any information or access BT requests without undue delay. This includes:

4.2.1.1 the Customer Contact details;

4.2.1.2 any health and safety rules and regulations and security requirements that apply at a Site;

4.2.1.3 the name and contact details for a Nominated Representative responsible for liaising with BT regarding the Vulnerability Notification and Patching Service Option. The Customer will advise BT if the Nominated Representative changes and ensure that BT has the current details of the Nominated Representative. The Customer will ensure that the Nominated Representative will:

(a) request implementation of Patches for each affected Security Appliance for the Vulnerability Notification and Patching Service Option;
(b) agree a time slot with BT for the implementation of such Patches;
(c) assess the suitability for deployment of the Patches that BT advises are available to address notified Vulnerabilities within the Customer's specific environments and for any post-implementation testing; and
(d) request and authorise that the Patch is reversed out in the event that the Patch introduces issues.

4.2.1.4 access to Site(s) during Business Hours, or as otherwise agreed, to enable BT to set up, deliver and manage the Service;

4.2.1.5 when the Customer selected a BT Takeover model and the Customer is transitioning the Customer's existing services to BT, the Customer will provide remote management access to the Customer Equipment and an inventory list with information relating to the Customer Equipment to be transitioned with relevant specifications, including:

(a) make and model of the Customer Equipment, and any hardware or software optional components;
(b) location of the Customer Equipment;
(c) serial numbers;
(d) software versions and licence information;
(e) network diagrams;
(f) Customer Equipment name and IP Addressing;
(g) details of any third party contracts, service level agreements and equipment; and
(h) details of the Customer's existing CSP(s);

Any changes to the inventory provided will be done by written agreement; whereby the Parties shall agree:

(a) the respective changes to the inventory;
(b) as changes to the inventory may cause delay to the transition of the Customer's service or the Operational Service Date; if applicable a new delivery date; and
(c) As changes may result in a change to the Charges to reflect the revised scope of the BT Service, if applicable any new Charges.

4.2.2 **Preparation**. The Customer will complete any preparation activities that BT may request to enable the Customer to receive the Service promptly and in accordance with any reasonable timescales. This includes:

4.2.2.1 **Customer IDs and passwords**; whereby the Customer will provide any account names and passwords necessary to install and commission the Service on BT Equipment or Customer Equipment. The Customer may request up to five (5) login/password combinations for access to the BT security portal, for use by the Customer or its agents. At the Customer's sole discretion, the Customer may assign one (1) login combination to BT personnel. The Customer is responsible for its agents' use of these IDs.

4.2.2.2 **Site planning guide;** as the Customer will be given a Site planning guide with details of the environmental requirements and sizing guides for the equipment being provided by BT; it is the Customer's responsibility to make sure the Site complies with this guide before service installation can proceed. Any defects will result in a delayed delivery date and Service Levels will not apply.

4.2.2.3 **Cooperation with surveys**; organised by BT as set out in Paragraph 3.2.2. Failure by Customer in co-operation with such surveys may result in a change to the Customer Committed Date and Charges for an aborted Site visit. BT will in such event provide a new quote to the Customer, detailing the additional Charges the Customer will need to pay for the additional work to be completed and a new proposed Customer Committed Date. Where the Customer,

(a) accepts the new quote, BT will either cancel the existing Order to the affected Site(s) and generate a new Order for the affected Site(s); or modify the existing Order to reflect the new requirements; or

(b) does not accept the new quote or the Customer does not instruct BT to proceed with the existing Order, BT will cancel the Customer's existing Order for the provision of the Service to the affected Site(s) as set out in the General Terms and Conditions and BT will have no obligation to provide the Service to that Site.

4.2.2.4 **additional work;** where the BT surveys as set out in Paragraph 3.2.2 identify that additional work is required to be undertaken by the Customer in order to provide a suitable environment, completing these works prior to installation of the Service;

4.2.2.5 **compatibility aspects;** where the Customer will ensure that the LAN protocols and applications the Customer use are compatible with the Service, conform to relevant industry standards, Customer's MPLS/Internet access circuit bandwidth is sufficient to meet the Customer's requirements and the requirement for in-band management access from BT. The Customer will provide written confirmation to BT upon request;

4.2.2.6 **IP Addresses;** whereby the Customer will manage and provide BT with accurate details of the Customer's internal IP Address design. The Customer will register any required Internet domain names using legitimate addresses which are public, registered and routed to the Customer's Site. The Customer's network and all applications on the Customer's side of the SMB must conform to all relevant IP standards. The Customer shall not use a Domain Name which infringes the rights of any person in a corresponding trade mark or name. The Customer shall not use IP addresses that it does not own or that are incorrectly specified. The Customer will be responsible for the use of these IP addresses;

4.2.2.7 **routing;** whereby the Customer will modify the Customer's network routing to ensure appropriate traffic is directed to the Security Appliance. The Customer acknowledges that switches provided as part of the Service only provide direct physical connectivity between Security Appliances and are not intended to support any network routing functionality;

4.2.2.8 **updates;** whereby the Customer will ensure that Security Appliances are able to receive updates, such as Vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose;

4.2.2.9 **Software support for Customer Equipment;** whereby the Customer will obtain and provide in-life support for any Software running on the Customer's Security Appliances. Where necessary, the Customer will provide and manage physical or virtual servers on the Customer's Site to a specification that BT agrees to run any Software that BT provides;

4.2.2.10 **Out of Band Access;** if an Out of Band Access modem is not included as part of the Service, the Customer will agree an appropriate alternative with BT to allow for fault diagnosis and base configuration, allowing BT to establish in-band control of the Security Appliance, at the time of installation and following a failure of the Security Appliance;

4.2.2.11 **Customer Equipment;** if BT has agreed to provide all or part of the Service using Customer Equipment, the Customer will ensure that the Customer Equipment is working correctly. If it is discovered to be faulty before the Operational Service Date:

(a) the Customer will be responsible for resolving any faults;
(b) BT will raise Charges to cover additional Site visits; and
(c) agreed installation dates and Customer Committed Date may no longer apply;

4.2.2.12 **CSP provisioning**. If the Customer has not ordered the CSP production Service Option from BT; the Customer will submit a CSP that meets the requirements and specifications advised by BT at least 28 Business Days before the envisaged Operational Service Date, including specifications that cover the Customer's legacy network, application services and other Enabling Services, using the CSP

requirements template. BT will respond with a security policy document, which will in turn be authorised by the Customer at least ten (10) Business Days before the envisaged Operational Service Date;

4.2.3 **Acceptance Tests.** After receiving notice from BT, the Customer will promptly carry out the Acceptance Tests for the Service. If the Service has not passed the Acceptance Tests due to severe faults, the Customer shall within five (5) Business Days notify BT in writing of such event. The Operational Service Date shall commence as set out in Paragraph 3.3 above.

4.3 **During Operation**

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

(a) ensure that Users report Incidents to the Customer Contact and not to the Service Desk;

(b) ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between BT and the Customer, and is available for all subsequent incident management communications;

(c) where the Customer has provided the Customer's own or a third party Enabling Service, ensure and confirm to BT that the Customer's own or a third party Enabling Service is working correctly before reporting Incidents to BT. BT will not record Downtime for reported Incidents until the Customer has provided this confirmation;

(d) inform BT timely of any planned works on any third party provided Enabling Service which may have an impact on the availability of the Service;

(e) retain responsibility for the CSP;

(f) provide service assurance support, where requested by BT, to progress Incidents for any Security Appliance installed onto an Enabling Service that has not been provided by BT;

(g) ensure that all Software provided is used solely for operation of the Service;

(h) monitor and maintain any Customer Equipment connected to the Service or used in connection with the Service and ensure that any such Customer Equipment is:

i. connected using the applicable network termination point, unless the Customer has BT's permission to connect by another means;

ii. technically compatible with the Service and will not harm or damage any Enabling Service, or any of BT's suppliers' or subcontractors' network or equipment; and

iii. approved and used in accordance with relevant instructions, standards and applicable law and any safety and security procedures applicable to the use of that Customer Equipment. In particular; the Customer shall, for any Customer Equipment used with the Service, be responsible for ensuring compliance with applicable law, including obtaining (if required) local import and User licenses and the written authority from all respective authorities, particularly for countries where the use and import of encryption Software and devices may be restricted by applicable law, or the export and re-export of the encryption Software or devices may be subject to the United States of America export control law and not act to misuse the Service as provided by BT to contravene or circumvent these laws. BT reserves the right to require the Customer to produce proof of compliance with such licensing and regulatory requirements. If the Customer cannot produce such proof to BT's satisfaction, BT reserves the right to suspend Service delivery or terminate for material breach as set out in the General Terms and Conditions.

(e) immediately disconnect any Customer Equipment, or advise BT to do so at the Customer`s expense, where Customer Equipment:

i. does not meet any relevant instructions, standards or applicable law; or

ii. contains or creates material that is in breach of applicable laws and the conditions of this Agreement and the Customer is contacted by BT about such material,

and redress the issues with the Customer Equipment prior to reconnection to the Service;

(f) distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' and the Customer`s access to the Service. If the Customer decides to, the Customer may assign one login combination to BT's personnel;

(g) be responsible for the Customer`s Users' use of access profiles and passwords;

(h) maintain a written list of current Users and provide a copy of such list to BT within five (5) Business Days following BT's written request at any time;

(i) ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Service and:

i. immediately terminate access for any person who is no longer a User;

ii. inform BT immediately if a User's ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;
iii. take all reasonable steps to prevent unauthorised access to the Service;
iv. satisfy BT's security checks if a password is lost or forgotten; and
v. change any or all passwords or other systems administration information used in connection with the Service if BT requests the Customer to do so in order to ensure the security or integrity of the Service;

(j) with regard to the permitted administrators for this Service;

i. request login/password combinations for access to a Customer Portal for use by the Customer or the Customer's agents. The Customer is responsible for its agents' use of these IDs. The Customer will – upon BT's request - assign one login combination to BT's personnel;
ii. ensure that the maximum number of administrators will not exceed five (5);
iii. not allow any administrator specific subscription to be used by more than one individual administrator unless it has been reassigned in its entirety to another individual administrator, in which case the Customer will ensure the prior administrator will no longer have any right to access or use the Service.

(k) will, where the Customer has selected the BT Owned, Customer Owned or BT Takeover delivery models and in the event of a failure of a Security Appliance, permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Security Appliance in its entirety and exchange it with a functioning replacement. BT will use reasonable endeavours to ensure any data on the recovered appliance or components is rendered unreadable prior to disposal or recycling; and

(l) will, for the BT Takeover delivery model, provide access to BT to any licence user centre, existing support contracts, authorisation code(s) or other information required by specific vendors and provided at the time of provision for registering products.

4.4 The End of the Service

On termination of the Service by BT or the Customer, the Customer will:

(a) provide BT with all reasonable assistance necessary to remove BT Equipment from the Site(s);
(b) promptly return or delete any confidential information that the Customer has received from BT during the term of the Agreement;
(c) disconnect any Customer Equipment from BT Equipment located at the Site(s);
(d) not dispose of or use BT Equipment other than in accordance with BT's written instructions or authorisation;
(e) arrange for any BT Equipment located at the Site(s) to be returned to BT; and
(f) be liable for any reasonable costs of recovery that BT incurs in recovering the BT Equipment.

5 Charges and Payment Terms

5.1 The Charges for the Service will comprise some or all of the following components, depending on the Service Options selected on the Order.

Pricing Component	One-time Charge	Recurring Charge	Notes
Security Appliances	Charges relating to the supply and installation of Security Appliances provided on an outright sale basis will be invoiced under separate conditions for the purchase of the Security Appliance.	Charges relating to the supply and installation of Security Appliances provided on a rental basis.	Different charges apply according to location and to different Security Appliances, depending on vendor and model.
Security Licenses	Charges relating to the supply of one-off or perpetual licences.	Charges relating to recurring licenses and supplier support contracts.	Charges vary, usually according to the number of the Customer's IP Addresses or Users.
Service Provision	Charges relating to project management and commissioning of the BT Managed Firewall Security Service.	N/A	Also applies to in-life changes to the BT Managed Firewall Security Service.

Pricing Component	One-time Charge	Recurring Charge	Notes
Service Management Fee	Set-up	Monthly Management	Covers provision and ongoing delivery of Service Options, including Out of Band management capability, Incident management and proactive monitoring of the BT Managed Firewall Security Service. Covers implementation of CSP change requests in accordance with the reasonable use policy set out in Paragraph 2.1.5.6.
Professional Services	Consultancy	N/A	Initial (optional) capture of CSP. Ad hoc consultancy as requested (charged on a per day basis).
Service De-Installation	De-Commissioning of the BT Managed Firewall Security Service.	N/A	Covers disconnection and removal of BT Equipment from the Customer's Site at end of Agreement.

5.2 The invoicing start date is the Operational Service Date except if the Customer requires BT to delay installation or configuration of Security Appliance for more than 30 days. In such event invoicing will start 30 days from the original planned installation date.

5.3 Installation Charges will be charged from the Operational Service Date or monthly in arrears prior to the Operational Service Date for any work carried out where the planned installation period is longer than one month.

5.4 In addition; BT will invoice the Customer:

5.4.1 any Charges as agreed in writing where the changes are outside the scope of the Service Management Fee; being changes to the CSP in excess of the "reasonable use" restrictions;

5.4.2 any Charges as agreed in writing for Emergency or Urgent Changes the Customer issued in error;

5.4.3 any Charges as agreed in writing for any refresh or upgrade of appliances or applications required by the Customer, unless the refresh or upgrade is operationally necessary to enable BT to continue to provide the BT Service. This does not apply to patching of applications or changes to the CSP;

5.4.4 any Charges as agreed in writing for any refresh or upgrade that is required as a result of capacity issues arising as a consequence of an increase in traffic or activation of new features;

5.4.5 any other Charges as agreed by Order (e.g. if Customer request information as set out in Paragraph 3.8.4);

5.4.6 any extra costs BT has incurred due to inaccuracies in information provided by the Customer to BT, including the requirements of the CSP or the provisions of Paragraph 4.2.1.5.;

5.4.7 any extra costs BT has incurred from a supplier for reinstating for the Customer any by the Customer lapsed support contracts or license agreements; and

5.4.8 any extra costs BT has incurred for having additional Site visits planned due to Customer failure to comply with its obligations. This may apply for Customer's failure to co-operate with surveys as set out in Paragraph 3.2.2. or for faulty Customer Equipment as set out in Paragraph 4.2.2.11.

6 Service Levels

The Service Levels set out in the General Service Schedule apply to the Service; except to CSP change requests, the Vulnerability Notification and Patching Service Option to which no Service Levels apply.

7 Data Processing

7.1 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 General Terms and Conditions of the Agreement and the relevant DPA (Data Processing Agreement) when applicable.

7.2 The nature and purpose of the Processing of Customer Personal Data by BT. With the BT Managed Firewall Security Service, BT:

(a) provides a service that allows the Customer to configure the Service implementing rules by which source and destination IP Addresses, protocols, Users and applications can be controlled via the CSP;

(b) monitoring traffic traversing the Service to enforce the rules and CSPs implemented on the Security Appliance;

(c) sharing Customer Personal Data with the suppliers of BT Equipment or Customer Equipment or sub-contractors as may be necessary for the provision and management of the Service including installation, maintenance and resolution of Incidents;

(d) if the Customer have selected the Threat Emulation Service, Customer Personal Data being sent automatically from Security Appliances or Software to cloud-based infrastructure operated by the supplier for threat emulation and assessment;

(e) accessing a log of customer IP Addresses, MAC addresses and Users, together with attempted URL and website visits by those addresses and Users, using an online Portal in order to provide the reports.

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

- website or IP Address of destination;
- IP Address of source device;
- MAC address of source device;
- business contact details including:
  i. name;
  ii. address;
  iii. telephone number;
  iv. email address;
  v. job title;
  vi. company name; and
- contact records.

7.4 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).