BT Managed Firewall Security (Fortinet)
Service Annex to the BT Managed Security Schedule

BT Contract Reference:
Customer Contract Reference (optional):

PARTIES:	The Customer	BT Spain
Name or Corporate name	XXXXXXXXXX (hereinafter referred to as "**The Customer**")	**BT GLOBAL ICT BUSINESS SPAIN, S.L.U.** (hereinafter referred to as "**The Provider**", "**Supplier**" or **"BT"**)
Fiscal Address	XXXXXXXXXX	C/ María Tubau Nº3 28050 Madrid
Tax ID/VAT	XXXXXXXXXX	B- 88625496
Company Representative	XXXXXXXXXX NIF of representative (ID Number) XXXXXXXXXXX Title: XXXXXXXXXXX	Paul Rhodes NIF of representative (ID Number): X0.688.132-H Title: Legal representative

BT Managed Firewall Security is an Associated Service under BT Managed Security Services. As result the conditions as set out in the BT Managed Security Schedule shall apply in addition to this Annex, except if explicitly stated otherwise in this Annex.

1 DEFINITIONS AND ABBREVIATIONS

The following definitions and abbreviations apply, in addition to those in the General Terms and Conditions and the BT Managed Security 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 as free of material faults and that the BT Managed Firewall Security 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.

"AD-VPN" or **"Active Directory VPN"** means a VPN type that allows to dynamically establish direct tunnels between spokes of a hub-and-spoke architecture.

"**Automated IOC Blocking**" has the meaning given in Paragraph 2.2.14 (b).

"Availability" means the period of time when the Service is working.

"BGP" means a network protocol designed to exchange routing and reachability information between autonomous systems.

"**BT Blocklist**" means any IOCs which BT has identified using its Eagle-I Platform.

"BT Managed Firewall Security" means the service as set out in this Annex. When BT Managed Firewall Security is used in conjunction with BT Managed Security Services this may also be referred to as "Service" overall;

"**BT Managed Security Service Schedule**" means the Schedule associated with BT Managed Firewall Security providing a range of graded security management services which can be used in association with, and as an overlay to the Service.

"**BT Owned**" means the delivery model for BT Managed Firewall Security where BT will provide, install and commission new Security Appliances as BT Equipment, including any hardware and Software, licensing and support agreements for the Security Appliances and will arrange for any on-Site support and remote service management as set out in Paragraph 2.1.1.

"BT Takeover" means the delivery model for BT Managed Firewall Security where BT will take over the management of existing Customer Security Appliances and whereby BT will arrange for any on-Site support and remote service management as set out in Paragraph 2.1.1.

"Co-operative Mitigation" has the meaning given in Paragraph 2.2.15.

"Contracted Maintenance Hours" means the times when BT shall provide maintenance for Security Appliances ordered as BT Equipment. These shall be Business Hours unless stated otherwise.

"**Customer Owned**" means the delivery model for BT Managed Firewall Security where - upon BT's recommendation- new Security Appliances will be ordered by the Customer as Customer Equipment and whereby BT will arrange for any on-Site support and remote service management as set out in Paragraph 2.1.1.

"Downtime" means the period of time during which a Qualifying Incident(s) exists.

"**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.

"**Eagle-I Enhanced Firewall Service**" means the Service Option specified at Paragraph 2.2.134.

"**Eagle-I Platform**" means the solution through which BT shall identify IOCs.
"**Enabling Service**" has the meaning given in Paragraph 4.1.2.
"**End of Life**" means any hardware or software that is no longer supported by the manufacturer, vendor or supplier and is incapable of cost-effective upgrade or update to a supported version. BT can only provide limited support if the hardware or software reaches this stage.
"**Ethernet**" means a family of computer networking technologies for LANs.
"Existing Blocklist Enhancement" has the meaning given in Paragraph 2.2.14 (a) (ii).
"**Firewall Intrusion Detection and Prevention Service**" means the Service Option as set out in Paragraph 2.2.3.
"FortiGate" means a next generation firewall, provided by Fortinet.
"**IOCs**" or "**Indicators of Compromise**" has the meaning given in Paragraph 2.2.14 (a) (i).
"**IPSec**" means IP security; it is a standards-based framework that provides layer 3 services for confidentiality, privacy, data integrity, authentication and replay prevention.
"IPSec Tunnel(s)" means either a static or dynamic virtual communication path between two end points that may be encrypted and have different levels of authentication to ensure the Customer has secure connectivity.
"Mitigation Action" means a recommended mitigating action which should be taken to address the impact of IOCs identified by BT.
"**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.
"**PSTN**" means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.
"**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.
"**Service Management Boundary**" has the meaning given in Paragraph 3.6.
"**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.
"**SSL**" means secure sockets layer.
"**SSL Encrypted Traffic**" means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

(a) HTTPS;
(b) SMTPS;
(c) POP3S;
(d) IMPAS; and
(e) FTPS.

"**SSL/TLS Inspection**" means the Service Option as set out in Paragraph 2.2.9.
"**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.
"**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.
"**Wide Area Network**" or "**WAN**" means the infrastructure that enables the transmission of data between Sites.

2 SERVICE DESCRIPTION

BT Managed Firewall Security 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" with options according to Customer requirements and is provided as an Associated Service with BT Managed Security Services as set out in the BT Managed Security Schedule. 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.

This BT Managed Firewall Security is for the moment only available with Security Appliances provided by BT's vendor Fortinet Inc.

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 Application licenses**. 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 **Delivery- Managed Installation**. BT 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) in accordance with the Graded Service Tier ordered by the Customer as further set out in the BT Managed Security Schedule.

2.1.4 **Incident Management**. BT will provide 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. The level of Incident Management depends on the Graded Service Tier ordered by the Customer as further set out in the BT Managed Security Schedule.

2.1.5 **Pro-active Monitoring**. BT will monitor the performance of the BT Managed Firewall Security as further set out in the BT Managed Security Schedule.

2.1.6 **Security Threat Intelligence.** BT will provide general intelligence bulletins and reports for BT Managed Firewall Security as further set out in the BT Managed Security Schedule.

2.1.7 **Service Performance Reports.** BT will provide near real-time or historic reports for key Service performance metrics, and for security-related events related to the BT Managed Firewall Security as further set out in the BT Managed Security Schedule.

2.1.8 **Signature Updates**. BT will identify and implement Signature Updates on the BT Managed Firewall Security as further set out in the BT Managed Security Schedule.

2.1.9 **Log Capture**. BT will implement a logging capability on the BT Managed Firewall Security depending of the Graded Service Tier as ordered by the Customer as further set out in the BT Managed Security Schedule.

2.1.10 **Licensing and Vendor Support Agreement Management**. BT will provide licensing and vendor support agreement management for the BT Managed Firewall Security as further set out in the BT Managed Security Schedule.

2.1.11 **Continuous Improvements with Review**. BT will provided Continuous improvements with review on the BT Managed Firewall Security depending of the Graded Service Tier as ordered by the Customer as further set out in the BT Managed Security Schedule.

2.1.12 **Vulnerability Management and Patching of Security Appliances**. BT will provided vulnerability management and patching on the BT Managed Firewall Security depending of the Graded Service Tier as ordered by the Customer as further set out in the BT Managed Security Schedule.

2.1.13 **Changes to the CSP**. BT will provide support for changes to the CSP. The level of BT support for changes to the CSP depends on the Graded Service Tier ordered by the Customer as further set out in the BT Managed Security Schedule. For BT Managed Firewall Security following shall apply in addition:

2.1.6.1 the following amount of change requests per Security Appliance are included in the Charges:

Change type	Foundation	Foundation Plus	Premium
Standard Change	six per month	eight per month	ten per month
Urgent Change	one per month	two per month	three per month

2.1.6.2 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;

2.1.6.3 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 are not included. The Customer:

(a) may order from BT Professional Services to advise the Customer what is exactly required; and

(b) Will agree the required changes by issuing a new Order.

2.2 Service Options

Following Service Options may be available subject to additional Charges and conditions as set out in the Order. Not all Service Options may be available across all vendors of Security Appliances.

2.2.1 **VPNs.**

(a) BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards:

(i) remote access IP Sec/SSL 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;

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

(iii) third party (extranet) IP Sec 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.

(b) Where the Customer provides the digital certificate to BT, as set out in the Order:

(i) BT will install it within seven days of receipt from the Customer.

(ii) BT will notify the Customer of the date of expiry of the digital certificate three months prior to the date of expiry. The Customer will advise BT, in writing, within one month of the date of BT's notification whether or not the Customer wants to renew its digital certificate;

(iii) if the Customer wants to renew its digital certificate, the Customer will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate; and

(iv) BT will not be liable for issues caused by expired digital certificates if the Customer does not confirm to BT that it wants to renew its digital certificate in; or the Customer does not provide BT with an up-to-date digital certificate.

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 (IPS):**

(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. 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) not be responsible for evaluating these signatures beforehand.

(b) BT will advise the Customer how the IPS that the Customer has selected operates with regard to alerting or IPS specific reporting;

(c) 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 **Additional Threat Emulation Service (only available if the Premium Graded Service Tier was ordered):**

(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 **SSL/TLS Inspection**

(a) BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP).

(b) BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.

(c) If the SSL/TLS Inspection Service Option is selected, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided the Customer's CSP permits such scanning.

2.2.10 **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.

2.2.11 **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.

2.2.12 **Ad Hoc technical support / Professional Service.** The Customer may order for Professional Services from BT as set out in the BT Managed Security Service Schedule.

2.2.13 **Eagle-I Enhanced Firewall Service**

BT shall provide the Customer with the Eagle-I Enhanced Firewall Service, subject to the requirements set out below.

(a) Existing Blocklist Enhancement

(i) Subject to BT confirming that Customer's Security Appliance is suitable for use with the Eagle-I Enhanced Firewall Service, BT will use its Eagle-I Platform to identify any unique malicious IPs and/or URLs to supplement Customer's Security Appliance's existing blocklist of malicious IPs and/or URLs ("Indicators of Compromise" or "IOCs".)

(ii) Upon confirming the suitability of Customer's Security Appliance, BT will add new IOCs to the BT Blocklist for consumption by Customer's Security Appliance ("Existing Blocklist Enhancement".)

(b) Automated IOC Blocking

(i) Subject to BT confirming the technical feasibility of applying Automated IOC Blocking to Customer's Security Appliance, as part of its remote service management of Customer's Security Appliance, BT shall automatically implement changes to Customer's Security Appliance so that it will block IOCs propagated from the BT Blocklist ("Automated IOC Blocking").

(ii) For the avoidance of doubt, when the Eagle-I Enhanced Firewall service is specified, subject to the requirements of technical feasibility (as outlined above at Paragraph 2.2.14(b)(i)), BT shall implement Automated IOC Blocking. By specifying the Eagle-I Enhanced Firewall Service, the Customer hereby consents to BT implementing Automated IOC Blocking in respect of Customer's Security Appliance.

(iii) BT shall not be responsible for any wider impact of any Automated IOC Blocking, including but not limited to any impact from the Automated IOC Blocking on Customer Equipment, or on Customer's wider network.

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:

3.2.1 provide the Customer with a target delivery date; which will – if the Customer has ordered Foundation Plus or Premium – be the Customer Committed Date for the purpose of measuring the On-Time Delivery Service Level;

3.2.2 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);

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

(a) 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

(b) 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;

3.2.4 provide the Customer with the Site Planning Guide;

3.2.5 appoint a named representative to be the Customer's single point of contact for the delivery of the Service; and

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:

3.4.1 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 Simple Changes as soon as reasonably practicable and they will typically involve individual lines of port/protocol, routing or network address translation changes. Any Complex Changes to the CSP not will incur additional Charges as agreed in an Order and may be scheduled for implementation following this five (5) Business Day period;

3.4.2 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;

3.4.3 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;

3.4.4 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;

3.4.5 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;

3.4.6 will respond and remedy any Incident reported by the Customer as set out in the BT Managed Security 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;

3.4.7 will notify the Customer if BT anticipates that Customer's hardware or software will become End of Life and as result will no longer be supported by BT under this Service. As part of this notification BT will recommend to the Customer the details of any required replacement or upgrade of applicable hardware or software, the respective timescales and the expected costs;

3.4.8 will, when the Customer selected BT Owned or BT Takeover delivery model, perform any changes (replacement or upgrades) to the hardware and/or Software during the Minimum Period of Service to avoid the hardware and Software would become End of Life; and

3.4.9 will, where Co-operative Mitigation with the Premium Graded Service Tier has been selected by the Customer, implement Mitigation Action as quickly as is technically practicable.

3.5 **The End of the Service.** On termination of the Service by either Party, BT will:

3.5.1 terminate any rights of access to the relevant BT Security Portal and relevant Software and stop providing all other elements of the Service;

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

3.5.3 delete any Content; and

3.5.4 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).

3.6 Service Management Boundary (SMB) and Exclusions.

3.6.1 BT will provide and manage the BT Managed Firewall Security as set out in this Annex and the BT Managed Security Schedule 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,

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

(a) issues on Users' machines, free downloadable vendor software not provided by BT, 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) managing identities of Users.

3.6.3 BT does not make any representations, whether express or implied,

(a) about whether the Service will operate in combination with any Customer Equipment or other equipment and software; or
(b) as to any outcomes of Automated IOC Blocking undertaken as part of the Eagle-I Enhanced Firewall Service Option, including but not limited to any reduction in security incidents or to the threat impact on any Customer Equipment or Customer's wider network.

3.6.4 about whether the Service will operate in combination with any Customer Equipment or other equipment and software.

3.6.5 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.

3.6.6 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.

3.6.7 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;

3.6.8 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;

3.6.9 Except if explicitly stated as forming part of the BT's responsibilities as set out in this Paragraph 3, BT will not be liable when the hardware and/or Software becomes End of Life and the Customer has not replaced or upgraded the respective hardware and/or Software in accordance with BT's recommendation as set out in Paragraph 3.4.12. In such event:

(a) BT will no longer be able to provide the Customer full support for such of End of Life hardware and/or Software and the Customer will receive a limited Service; and
(b) the Service Levels shall no longer apply;

3.6.10 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

3.6.11 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.

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

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

4 THE CUSTOMER'S RESPONSIBILITIES

4.1 Prerequisites

4.1.1 Enabling Service

4.1.1.1 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,

4.1.1.2 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.

4.1.2 Import and Export

4.1.2.1 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.

4.1.2.2 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.

4.1.2.3 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.

4.1.3 **Obligations when ordering Co-operative Mitigation.**

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

(a) agree in the Order that BT is authorised to not take Mitigation Action in relation to specific security controls, and where appropriate specific endpoint Devices or End-User Identities;
(b) select in the Order if such is done either automatically or subject to Customer's approval; and
(c) securely provide BT with the necessary access credentials to the platforms that are used by the Customer to make policy changes to the endpoints or End-User Identities requiring Co-operative Mitigation and notify BT of any subsequent changes to these credentials.

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 **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.

4.2.2.2 **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.

4.2.2.3 **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;

4.2.2.4 **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;

4.2.2.5 **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;

4.2.2.6 **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;

4.2.2.7 **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;

4.2.2.8 **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;

4.2.2.9 **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;

4.2.3 **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:

4.3.1 ensure that Users report Incidents to the Customer Contact and not to the Service Desk;

4.3.2 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;

4.3.3 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;

4.3.4 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;

4.3.5 retain responsibility for the CSP;

4.3.6 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;

4.3.7 ensure that all Software provided is used solely for operation of the Service;

4.3.8 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:

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

(b) 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

(c) 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.

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

(a) does not meet any relevant instructions, standards or applicable law; or

(b) 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;

4.3.10 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;

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

4.3.12 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;

4.3.13 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:

(a) immediately terminate access for any person who is no longer a User;

(b) 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;

(c) take all reasonable steps to prevent unauthorised access to the Service;

(d) satisfy BT's security checks if a password is lost or forgotten; and

(e) 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;

4.3.14 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;

4.3.15 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;

4.3.16 will; when hardware and/or Software would become End of Life; be responsible to timely order and/or implement any changes as recommended by BT in accordance with Paragraph 3.4.12 which depending on the selected delivery model will entail:

(a) in the event the Customer selected the Customer Owned delivery model; the Customer shall at all times be fully responsible for doing such replacement or upgrade and paying any related expenses; or

(b) in the event the Customer selected the BT Owned or BT Takeover delivery model and the Customer would like to continue with the Service after the expiration date of the Minimum Period of Service; the Customer shall order from BT any changes required to avoid such hardware and/or Software becomes End of Life;

4.3.17 where the Eagle-I Enhanced Firewall Service Option is specified, BT will implement any changes as part of Automated IOC Blocking as quickly as is technically practicable; and

4.3.18 when the Customer orders the Co-operative Mitigation option with Premium Graded Service Tiers; will inform BT of any changes concerning specific endpoint Devices or End-User Identities to which BT is authorised to take Mitigation Action.

4.4 **The End of the Service.**

4.4.1 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.

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

(a) the Customer shall notify BT whereafter BT will confirm the date from which the Mitigation Action component will be de-activated from the Service;

(b) the Customer shall remove BT's access credentials to endpoint Device or End-User Identities;

(c) the Customer shall from the date of de-activation be responsible for implementing any Mitigation Action which BT recommends; and

(d) for the avoidance of doubt, deselection of the Co-operative Mitigation component of the Service shall not result in any reduction to the Charges which are payable in line with the selected Service Tier.

5 CHARGES AND PAYMENT TERMS

5.1 The Charges for the Service will, depending on the Service Options and Graded Service Tier selected, be set out on the Order.

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 for changes to the CSP in excess of the "reasonable use policy";

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 3.5.4 or changes to avoid hardware and/or Software would become End of Life as set out in Paragraph 4.3.16);

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

6.1 **On-Time Delivery**. If the Customer orders Foundation Plus or Premium as BT Managed Security Service; the On-Time Delivery Service Level as set out in the BT Managed Security Schedule shall apply.

6.2 **Availability**. The following Availability Service Level shall apply:

6.2.1 BT will assign an availability category ("SLA Category") determined by the Security Appliance configuration and Site location. This will be stated on the Order. Each SLA Category has an associated Annual Performance Target (APT), which is used to calculate the APT Downtime. BT will count Downtime for each properly reported Qualifying Incident and will keep a record of cumulative Downtime by Site, in units of full minutes, for each Month and the SLA Year. If cumulative Downtime in a Month exceeds the Service Credit Start Point (SCSP), the Customer may claim a Standard Service Credit(s) as shown in the table below, for each affected Site up to a maximum of one month's Recurring Charges for an affected Site. If the cumulative Downtime in any SLA Year (or portion of a SLA Year for Sites installed for less than a SLA Year) exceeds the APT Downtime BT will apply the Elevated Service Credit(s) shown in the table below for all valid claims until the cumulative Downtime in the SLA Year falls below the APT Downtime. During this time the SCSP will be immediate for all SLA Categories.

6.2.2 Unless otherwise stated Service Credits apply to each started hour of Downtime above the SCSP.

SLA Category	Annual Performance Target (APT)	APT Downtime	SCSP for Standard Service Credits	Standard Service Credits	Elevated Service Credits
Cat A++	=>99.999%	5 minutes	immediate	4% of Site Charges for each started 5 minutes of Downtime above the SCSP	8% of Site Charges for each started 5 minutes of Downtime
Cat A+	=>99.99%	1 hour	immediate	4% of Site Charges for each started 15 minutes of Downtime above the SCSP	8% of Site Charges for each started 15 minutes of Downtime
Cat A1	=>99.97%	3 hours	immediate	4% of Site Charges	8% of Site Charges
Cat A	=>99.95%	4 hours	immediate	4% of Site Charges	8% of Site Charges
Cat B	=>99.90%	8 hours	1 hour	4% of Site Charges	8% of Site Charges
Cat C	=>99.85%	13 hours	3 hours	4% of Site Charges	4% of Site Charges
Cat D	=>99.80%	17 hours	5 hours	4% of Site Charges	4% of Site Charges
Cat E	=>99.70%	26 hours	7 hours	4% of Site Charges	4% of Site Charges
Cat F	=>99.50%	43 hours	9 hours	4% of Site Charges	4% of Site Charges
Cat G	=>99.00%	87 hours	11 hours	4% of Site Charges	4% of Site Charges
Cat H	=>98.00%	175 hours	13 hours	4% of Site Charges	4% of Site Charges
Cat I	=>97.00%	262 hours	15 hours	4% of Site Charges	4% of Site Charges

6.2.3 Downtime is measured from when a Qualifying Incident is reported to BT's Service Desk and ends when BT

clears the incident. The Customer will be given an Incident report reference number ("trouble Ticket" number) for each properly reported Incident.

6.2.4 BT will inform the Customer when the Qualifying Incident is cleared, and will close the trouble Ticket when either the Customer confirms within 1 hour that the Incident is cleared, or BT has attempted and failed to contact the Customer and the Customer does not respond within 1 hour. If the Customer confirms that the Incident is not cleared within 1 hour of being informed, the trouble Ticket will remain open, and Downtime adjusted.

6.2.5 Downtime will only be measured during the Contracted Maintenance Hours as specified on the Order.

6.2.6 The following are not Qualifying Incidents, and Downtime will not be measured;

(a) if the Customer asks BT to test the Service although no Incident has been detected and/or reported;
(b) if the Service has been modified or altered in any way by the Customer or at the Customer's request;
(c) during Planned Maintenance;
(d) for Incidents due to any Customer performed network configurations not approved by BT;
(e) for changes or alterations made other than by BT to the Service or to BT Equipment, connections, routing plan, applications or test equipment, or the mapping of applications; or
(f) if an Incident is reported and BT cannot confirm that an incident exists after performing tests.

6.3 **Restore-Time (Resilience).** If the Customer orders the High Availability solution as a Resilient Service to a Site, then if either the primary or secondary Security Appliance fails and BT does not restore Service to both Security Appliances within 24 hours of the Customer reporting or BT detecting the failure, ('the initial 24 hours") BT will give the Customer a Service Credit for valid claims. The Service Credit will be 1% of the monthly Recurring Charges for the affected Site for each started hour after the initial 24 hours up to a cap of 100% of the monthly Recurring Charges for the affected Site. As Service is available during this period this time will not count towards Downtime. This Service level only applies if the Security Appliances are ordered with 24/24hours – 7/7 days maintenance which may not be available in all locations.

6.4 **Exclusions.** Next to the general Service Level exclusions as set out in BT Managed Security Schedule; above Service Levels shall also no longer apply when the hardware and/or Software becomes End of Life and is not replaced as set out in this Annex.

6.5 **Claiming of Service Credits.** The conditions for claiming Service Credits are set out in the BT Managed Security Schedule.

7 MINIMUM PERIOD OF SERVICE, TERMINATION, RENEWAL AND CHANGES

7.1 **Minimum Period of Service**. Unless otherwise agreed on an Order, the Minimum Period of Service will be a period of twelve (12) consecutive months beginning on the Operational Service Date.

7.2 **Termination and Renewal**. At ordering the Customer shall select on the Order for each Service if the Customer prefers auto-renewal or not.

7.2.1 In the event auto-renewal was selected by the Customer; the Service shall at the end of the Minimum Period of Service or each subsequent Renewal Period be automatically renewed for a Renewal period of 12 months; except if the Customer has terminated the Service at least 90 days before the expiry date of the Minimum Period of Service or an ongoing Renewal Period.

7.2.2 In the event no auto-renewal was selected by the Customer; the Service shall end automatically at the end of the Minimum Period (or a subsequent Renewal Period) unless the Parties agree to renew the Service - by signature of a new Order - with a Renewal Period at least 90 days before the expiry date of the Minimum Period of Service or an ongoing Renewal Period.

7.2.3 In addition Customer may at any time early terminate the Service for convenience in accordance with following conditions:

(a) the Customer will provide advance notice to BT in accordance with the termination provisions as set out in the General Terms and Conditions;
(b) next to any outstanding Charges until the day of termination, the Customer shall pay BT termination fees as compensation, equal to:
(i) any waived Installation Charges as set out on the Order;
(ii) de-installation Charges as set out on the Order. If no de-installation Charges are set out on the Order the de-installation Charges shall be equal to the Installation Charges;
(iii) any charges reasonably incurred by BT from a supplier as a result of the early termination including any charges in respect of software licences or vendor support agreement;
(iv) for any parts of the Service that were terminated during the first 12 months of the Minimum Period of Service:

- 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service;
- 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service with the exception of the Recurring Charges for the Security Appliances provided on a rental basis which will be 100 per cent of the Recurring Charges; and

(v) for any parts of the Service that were terminated after the first 12 months of the Minimum Period of Service or during a Renewal Period, 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service or the Renewal Period with the exception of the Recurring Charges for the Security Appliances provided on a rental basis which will be 100 per cent of the Recurring Charges.

(c) termination charges for BT Managed Security Services will be calculated on the Recurring Charges after any discount has been applied and for BT Managed Firewall Security before any discount has been applied; and

(d) If the Customer has paid the charges or fees for the software licence or vendor support agreement in advance, the Customer may not be entitled to a refund of the charges for the remaining months of the Minimum Period of Service or Renewal Period.

7.3 **Changes**. In the event that both Parties wish to continue to supply and use the Service, BT may propose changes to the BT Managed Security Schedule, this Annex, the Charges and/or the General Terms and Conditions in accordance with following conditions:

7.3.1 BT will give the Customer at least 60 days prior written notice before the end of the Minimum Period of Service and each Renewal Period with detailed explanation of the required Change(s);

7.3.2 any changes will be agreed in writing between the Parties within 30 days after receipt of BT's notice to amendment;

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

(a) BT will continue to provide the Service; and

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

7.3.4 in the event the Parties cannot agree on the required changes; the Service shall end and BT will cease delivering the Service at the time of 23:59 on the last day of the Minimum Period of Service or the subsequent Renewal Period, as applicable.

8 DATA PROCESSING

9.1 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.

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

9.3 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.

9.4 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).

Simple and Complex Changes

Note: Any change not qualified in below table as "Simple" will be a Complex Change.

Simple Service Changes	
Change	**Mechanism for Requesting Changes**
Firewall Changes [AMF] – Set Permissions allowing Ip Addresses or IP range (Specific ports or all ports)	MyAccount – BT Change Manager
NAT (Simple) [AMF] – Simple NAT (Static NAT, 1 to 1 mapping)	MyAccount – BT Change Manager
NAT (Hide NAT) [AMF] - Hide NAT	MyAccount – BT Change Manager
NAT (Manual) [AMF] – Manual NAT	MyAccount – BT Change Manager
Firewall Routing [AMF] - Routes to Networks not directly connected to FW.	MyAccount – BT Change Manager
Proxy Rule Changes [AMF] – Modify proxy server internet access rules	MyAccount – BT Change Manager
URL Blacklisting/Whitelisting Changes [AMF] Block/Allow websites based on company business requirements.	MyAccount – BT Change Manager
Proxy Routing Requirements [AMF] Routes to Networks not directly connected to the proxy	MyAccount – BT Change Manager

In witness whereof, the Parties execute this document electronically, been effective from the date of the second signatory.

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