BT Managed Firewall/Web Security
Schedule to the General Terms

Contents

A NOTE ON 'YOU'

'You' and 'your' mean the Customer.

Phrases that refer to 'either', 'neither', 'each of us', 'both of us' 'we each' or 'we both' mean one or both BT and the Customer, whichever makes sense in the context of the sentence.

Part A – The Service

1 SERVICE SUMMARY

1.1 BT will provide you with BT's global Managed services, comprising:

1.1.1 the Standard Service Components; and

1.1.2 any of the Service Options that are selected by you as set out in any applicable Order,

(the "**Service**").

1.2 You may order:

1.2.1 BT Managed Firewall Security service; or

1.2.2 BT Managed Web Security service.

1.3 The Service controls inbound Internet traffic according to controlled exceptions, manages Users' outbound Internet access according to pre-defined policy and scans Internet traffic to block malware.

1.4 Where you select BT Managed Firewall/Web Security Service under the Managed Service from BT:

1.4.1 Paragraph 12.2.2 of this Schedule will not apply and in such case Paragraph 11 of Managed Service from BT Schedule to the General Terms will apply;

1.4.2 Part C of this Schedule will not apply and in such case Part C of Managed Service from BT Schedule to the General Terms will apply.

1.5 Where you select BT Managed Firewall/Web Security Service under a Managed Service:

1.5.1 Paragraph 12 of this Schedule will not apply and in such case Paragraph 4 of the Managed Service Schedule to the General Terms will apply.

2 STANDARD SERVICE COMPONENTS

BT will provide you with all of the following standard service components ("**Standard Service Components**") in accordance with the details set out in any applicable Order:

2.1 **Security Appliances**

2.1.1 You may choose from a range of Security Appliances or BT may recommend a Security Appliance as part of the overall Service design.

2.1.2 You may request to use Customer Equipment for the Service and BT may agree to such a request, subject to an assessment by BT that the Customer Equipment is suitable for use with the Service. This assessment will be carried out once you have provided the required information as set out in Paragraph 7.1.1 and BT will provide written confirmation that BT is able to support the Customer Equipment.

2.1.3 You will select one of the following Service delivery models:

(a) 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 ("**BT Owned**");

(b) you will provide the Customer Equipment to BT's specification. BT will provide the BT Equipment and arrange applicable licensing and support agreements as set out in the table at Paragraph 2.1.4 and will renew those agreements when required. BT will install and commission that BT Equipment and Customer Equipment, and will provide on-Site support and remote service management. If there is a fault in the Customer Equipment, BT will raise the necessary support requests on your behalf. You will retain ownership of all Customer Equipment ("**Customer Owned**");

(c) subject to Paragraph 2.1.2, BT will remotely manage existing Customer Equipment. BT will arrange applicable licensing and support agreements and will renew those agreements when required. If there

is a fault in the Customer Equipment, BT will raise the necessary support requests on your behalf. You will retain ownership of the Customer Equipment ("**BT Takeover**"); or

(d) you will provide and install any Customer Equipment, including hardware, software and applicable licensing and support agreements. BT will commission the equipment and provide remote service management and notify you of any failure in the Customer Equipment that BT detects. You will retain ownership of all Customer Equipment ("**Service Wrap Only**").

2.1.4 The table below sets out the responsibilities of both of us for the supply and management of Security Appliances, unless otherwise specified in the Order Form:

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

2.2 **Project Managed Installation**

BT's project manager will coordinate the Service installation and commissioning, in accordance with the Service delivery model you choose, liaising with you, installers and equipment suppliers as appropriate, depending on whether BT Equipment or Customer Equipment is being used. All project management activity will be administered remotely and the named representative will not visit your Site.

2.3 **Incident Management**

BT will provide a 24x7x365 Service Desk to respond to Incidents, in accordance with Paragraph 10.

2.4 **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 you.

3 SERVICE OPTIONS

3.1 BT will provide you with any of the following Service Options that are set out in any applicable Order and in accordance with the details set out in that Order:

3.1.1 **IPSec VPN:**

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

(i) Site to Site VPNs between two Security Appliances which are both owned by you and managed by BT;

(ii) remote access VPNs, for remote users to gain secure access to your internal network. BT will implement your rules to authenticate against your authentication server. You are responsible for providing and managing your own end-user VPN software; and

(iii) Third party (extranet) VPNs, for creating a site-to-site VPN between your Security Appliance managed by BT, and a Security Appliance owned or manged by you or a third party. BT will only deliver VPNs to Security Appliances managed by a third party after the Service Start Date.

3.1.2 **De Militarized Zones (DMZs):**

(a) BT will provide additional LAN segment interfaces on the Security Appliance, or on an adjacent network switch, according to your requirements.

(b) This is subject to there being sufficient physical ports available; additional Charges will apply if additional hardware is required to provide the interface.

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

(a) BT will:

(i) monitor traffic passing through your 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;

(iii) not be responsible for evaluating these signatures beforehand;

(iv) where "**bronze level services**" is selected in the Order, block high impact or high confidence attacks, as defined by the supplier of the Software used to deliver the 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 you advise BT of a conflict with any of your legitimate business traffic; and

(v) where "**platinum level services**" is 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 you as soon as practical and ask you if you wish to block the traffic causing the alert. BT will not proactively initiate this block in the absence of your instructions. BT will provide incident reports as part of this Service Option via the relevant Customer Portal.

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

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

(a) BT will:

(i) block access to those Internet sites that you ask BT to, in accordance with your CSP. Internet sites are arranged into groups which are regularly updated. You 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 your acceptable use policy (or similar warning). Upon acceptance, the page will be delivered;

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

(iv) if the SSL Control Service Option is selected, BT will also apply this service to HTTPS websites.

(b) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.8.

3.1.5 **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) If the SSL Control Service Option is selected, BT will also apply this service to files delivered via HTTPS websites.

(d) This Service Option does not include reporting as standard. Reporting may be available in accordance with Paragraph 3.1.8.

3.1.6 **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.

3.1.7 **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 you select, you 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 your Security Appliances.

(c) If a file has been 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 you require the Service to protect against malware contained within SMTP (email) attachments, you will arrange for your DNS MX 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 your email server.

(f) Submission and Processing of your data via BT's services will be at your sole discretion and at your own risk. Other than BT's obligations in Clause 14 of the General Terms, BT assumes no responsibility or liability for the receipt and Processing of such data.

3.1.8 **Security Event Reporting:**

(a) BT will:

(i) provide reporting facilities, either on-line or on a server hosted on your Site, which allows analysis of security-related events; and

(ii) not pro-actively view your 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 you are only provided with access to your 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.

3.1.9 **SSL Control:**

(a) BT will intercept and unencrypt SSL / Transport Layer Security (TLS) / HTTPS 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) You will provide BT with an up to date, digital certificate that may be installed on the Security Appliance. BT will install renewed digital certificates within seven days of receipt from you. BT will not be liable for issues caused by expired digital certificates.

3.1.10 **Checkpoint Capsule:**

(a) BT will:

(i) provide a non-exclusive, non-transferable, non-assignable right to access a shared, cloud based firewall and client Software that diverts Internet traffic from the User's laptop computer to that firewall, where protection is applied in accordance with your CSP for the number of purchased Users; and

(ii) provide access to a Customer Portal, where you may download the client Software and define your Users who are to be protected by the Service.

(b) You are responsible for distributing the client Software, installing it on the Users' laptops and enforcing compliance with its use.

(c) If identity-aware policies are to be applied, BT will provide you with access to Software which interacts with your active directory authentication server. You will be responsible for installing this on a suitable server within your internal network environment, such that this Software may access both the active directory server and the Internet. The use of the cloud-based firewall means that your information and data may be Processed in a country other than that where the User is located, and this country may be changed by BT.

3.1.11 **Instant messaging control (IM):**

(a) BT will configure the Security Appliance to provide control over IM communications made over common, specific, IM clients.

(b) Communications made using non-supported IM clients cannot be controlled using this service.

(c) BT will apply the following control measures if selected by you:

(i) global permit/deny of file transfers within IM;

(ii) controlling access to IM for specific user groups or IP addresses including time of day;

(iii) limiting the bandwidth allocation for IM traffic by speed or percentage allocation; and

(iv) selection and specification of warning text to Users that their IM sessions are being logged.

(d) BT will not antivirus check files transferred via IM.

3.1.12 **Media streaming control:** controlling User access and optimising voice and video media streams.

(a) BT will configure the Security Appliance to control incoming media streams and thereby limit the impact on your bandwidth. The service can limit the bandwidth available for media streaming traffic, and restrict access to media streaming for specific user groups or IP addresses including time of day.

(b) Specific media streaming versions and formats are supported, as specified in the data sheet for the applicable Security Appliance. Streams using a non-supported format will not be controlled.

3.1.13 **Identity Awareness / User groups:**

(a) BT will configure the Security Appliance to apply policy according to the authenticated identity of the User rather than just their IP address.

(b) This may require client Software to be installed within your network or on end-user devices, or ensuring BT has remote, read-only, access to your Active Directory authentication server.

(c) You will maintain the authentication database of users, groups and any access credentials that you require.

3.1.14 **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 you as set out in Paragraph 2.1.4. If it is your responsibility to provide the additional switches, we will advise you of number and type of switches required.

(d) Depending on the Security Appliances used and your 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.

3.1.15 **Ad Hoc 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.

3.1.16 **CSP production:**

BT will provide professional services to assist you in the production and implementation of your CSP for a period of three Business Days. If additional time is required for the creation of the CSP, this will be charged for as set out in Paragraph 11.2.2.

3.1.17 **Vulnerability Notification and Patching:**

(a) BT will identify, test and implement Patches for High and Critical CVSS in accordance with your authorisation;

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

3.2 The Service may not be available in all locations and Service Levels may vary depending on Site location.

3.3 Services Options may not be available on all Security Appliances. BT is not responsible if BT is unable to deliver the Service because of a lack of capacity on your selected Security Appliances.

3.4 BT cannot guarantee that the Service Options will operate without Incident or interruption or to intercept or disarm all malware.

4 SERVICE MANAGEMENT BOUNDARY

4.1 In addition to the Services that we offer as set out in Paragraph 2.1.3 for the Service delivery model you select, BT will provide and manage the Service as set out in Parts B and C of this Schedule and as set out in the Order up to the Service Management Boundary. Depending on the Service that you select, Paragraph 4.1.1 or Paragraph 4.1.2 will apply.

4.1.1 **BT Managed Firewall Security Service Boundary**

Internet / WAN side	Cable connecting firewall to your Router
LAN side	Ethernet port(s) on firewall or the switch provided by BT
Analogue exchange Line	Cable connecting BT's provided modem to PSTN socket

4.1.2 **BT Managed Web Security Service Boundary**

Internet / WAN side	Cable connecting proxy appliance to Security Appliance or your DMZ switches if present
LAN side	Ethernet port(s) on proxy appliance or BT's provided switch
Analogue exchange Line	Cable connecting BT's provided modem to PSTN socket

("**Service Boundary**").

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

4.2.1 issues on Users' machines or your servers (e.g. operating system, coding languages and security settings);

4.2.2 end to end network connectivity (e.g. your network or Internet connectivity); or

4.2.3 identity source management.

4.3 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.

5 ASSOCIATED SERVICES AND THIRD PARTIES

5.1 You will have the following services in place prior to the Service being delivered. You will ensure that these services meet the minimum technical requirements that BT may specify:

5.1.1 Internet connectivity;

5.1.2 WAN connectivity;

5.1.3 PSTN direct exchange line, to enable Out of Band Access management;

5.1.4 LAN / DMZ connectivity and associated infrastructure;

5.1.5 PSTN connectivity; and

5.1.6 broader IT environment, including the Security Appliances where they are your responsibility as set out in Paragraph 2.1.4, including authentication services, additional switches where required as set out in Paragraph 3.1.14(c), server / client platforms, security incident and event management (SIEM) solutions,

(each an "**Enabling Service**").

5.2 If BT provides you with any services other than the Service (including any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms and conditions.

6 SPECIFIC TERMS AND CONDITIONS

6.1 **Termination for Convenience**

For the purposes of Clause 17 of the General Terms either of us may, at any time after the Service Start Date and without cause, terminate the Service or any Order by giving 90 days' Notice to the other.

6.2 **Minimum Period of Service**

6.2.1 Unless one of us gives at least 90 days' written Notice to the other of an intention to terminate the Service at the end of the Minimum Period of Service, BT will continue to provide the Service and both of us will perform each of our obligations in accordance with the Contract.

6.2.2 If one of us gives at least 90 days' written Notice to the other of an intention to terminate the Service at the end of the Minimum Period of Service, BT will cease delivering the Service at 23.59 on the last day of the Minimum Period of Service.

6.3 **EULA**

6.3.1 You acknowledge that aspects of the Service may only be provided by BT if you have entered into an end user licence agreement ("**EULA**") with the supplier of BT Equipment or Customer Equipment as may be amended or supplemented from time to time by the supplier.

6.3.2 By accepting the terms of the EULA you acknowledge the relevant conditions and agree to observe and comply with them for any and all use of the Service.

6.3.3 You accept responsibility in accordance with the terms of the EULA for the use of the Software. You will follow all instructions given to you by the supplier.

6.3.4 You acknowledge that you enter into the EULA for your own benefit and that the rights, acknowledgements, undertakings, warranties and indemnities granted under the EULA are between you and the supplier only. BT does not grant you any rights from, or make any warranties to you about, the terms of the EULA.

6.3.5 You will report any breach or suspected breach of the EULA to the supplier directly as soon as you become aware of it.

6.3.6 Any loss or damage suffered by you or the supplier under the EULA will be enforceable only between you and the Supplier, and will not be enforceable against BT.

6.4 **Changes to the CSP**

6.4.1 Where you require a change to your CSP, for example as a result of changes to your application requirements or network environment, you may request additions, deletions, or modifications to your CSP and BT will provide you with the means to request Standard Changes or Urgent Changes to the CSP, either on the relevant Customer Portal or to the Service Desk. BT will charge you for this Service as set out in Paragraph 6.4.4 below.

6.4.2 You will order separately any changes to the Service that are required that involve physical changes to the Service, including Security Appliance upgrades and LAN re-arrangements. The CSP changes described in Paragraph 6.4.1 refer only to requests to change the rule-sets that define the Service's operation.

6.4.3 BT will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested CSP changes and advise you appropriately and will not be liable for any consequence arising from:

(a) your miss-specification of your security requirements in the CSP; or
(b) unforeseen consequences of a correctly specified and correctly implemented CSP.

6.4.4 BT will charge you for changes to the CSP within its Annual Service Management Fee.

6.4.5 BT will only make configuration changes as set out in Paragraph 6.4.1. 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 you professional services in accordance with Paragraph 3.1.15; or
(b) agree a change to the Contract that will only be effective if in writing and signed by both of us.

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

(a) if you are paying a Fixed Annual Price you will not raise Standard Change requests more frequently than five per month per firewall. Urgent Changes will not exceed one per month. The number of Urgent Changes raised will be measured by BT as an average over a rolling period of three months, per CSP. Where BT's measurements show that change requests are being raised more frequently than five per month, BT may, either:

(i) aggregate your requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays; or
(ii) review your requirements and agree with you an appropriate alternative implementation process and any associated charges.

There is no limit to the number of lines of changes that can be submitted at one time, however, only the first five lines will be completed within the target times.

(b) BT reserves the right to charge you for Emergency or Urgent Charges you issued in error or in excess of the "**reasonable use**" restrictions.

(c) access to the BT Customer Portal is controlled and will not be shared by your 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 unattended unlocked computer;

(iii) submit any unauthorised changes; or
(iv) attempt to access data that they are not authorised to access.

Customer Contacts are required to report the loss of any tokens or compromised passwords to within their own organisation and to BT immediately.

7 SERVICE TRANSITION

7.1 If you select the BT Takeover Service delivery model and you are transitioning your existing services to BT, you will provide any information or access BT reasonably requests, including:

7.1.1 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; and
(g) details of any third party contracts, service level agreements and equipment; and

7.1.2 remote management access to your Customer Equipment.

7.2 Any changes to the inventory provided in accordance with Paragraph 7.1.1 will be managed by written agreement and:

7.2.1 may cause delay to the transition of your service or the Service Start Date; and

7.2.2 may result in a change to the Charges to reflect the revised scope of the Service.

7.3 If a supplier charges BT to reinstate any lapsed support contracts or license agreements, these charges will be passed to you.

Part B – Service Delivery and Management

8 BT'S OBLIGATIONS

8.1 **Service Delivery**

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

8.1.1 will provide you with contact details for the service desk that you will be able to contact to submit service requests, report Incidents and ask questions about the Service ("**Service Desk**");

8.1.2 will comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at a Site and are notified to BT in writing. BT will not be liable if, as a result of any such compliance, BT is in breach of any of BT's obligations under this Contract;

8.1.3 will, once the requirements of the Service have been confirmed and agreed, and, where applicable, you provide the details set out in Paragraph 7.1, provide you with a date on which delivery of the Service (or each part of the Service, including to each Site) is due to start ("**Customer Committed Date**") and will use reasonable endeavours to meet any Customer Committed Date;

8.1.4 in the event that a change to the Service is required at any time before the Service Start Date, will produce a new quote to reflect your new requirements. If you:

(a) accept the new quote, BT will either:

(i) cancel the existing Order to the affected Site(s) and generate a new Order for the affected Site(s), with a new Customer Committed Date; or

(ii) modify the existing order to reflect the new requirements and provide a new Customer Committed Date;

(b) do not accept the new quote, you may instruct BT to proceed with the existing order; or

(c) do neither, BT will cancel your existing Order for the provision of Service to the affected Site(s) and BT will have no obligation to provide the Service to that Site and you acknowledge that where BT has ordered equipment to fulfil BT's obligations for an Order that is subsequently cancelled or amended and BT is unable to return the equipment to the supplier, the costs of such equipment will remain payable by you;

8.1.5 will:

(a) if you select the BT Owned Service delivery model, 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 you select the Customer Owned Service delivery model, 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;

8.1.6 will provide you with the Site Planning Guide;

8.1.7 will, where applicable, arrange for any surveys to be conducted to confirm the availability of a suitable environment for provision of the Services. If the surveys identify that additional work is required to be undertaken by you in order to provide a suitable environment, you will complete these works prior to installation. Failure to do so may result in a change to the Customer Committed Date, Charges for an aborted Site visit, or BT may provide a new quote to you in accordance with Paragraph 8.1.4;

8.1.8 will appoint a named representative to be your single point of contact for BT's project management Service Option, as set out in Paragraph 2.2; and

8.1.9 will validate that you have ordered the correct number of licenses to serve your requirements, in accordance with vendor commercial terms and according to information provided by you and:

(a) if BT determines that you have not ordered sufficient licences, BT will notify you and you will seek to rectify the situation within 30 days of the date of notification;

(b) if the situation is not resolved within this time BT may suspend the Service and subsequently terminate the Service in accordance with Clause 18 of the General Terms; and

(c) in any event, BT is not liable for unknown breaches of vendor commercial terms, where BT is acting on information provided by you.

8.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

8.2.1 contact you and agree installation date(s), including access for third party installers;

8.2.2 install the BT Equipment (if you select BT Owned or, where applicable, Customer Owned) or Customer Equipment (if you select Customer Owned). Once installed, BT will configure the Service remotely in accordance with your CSP;

8.2.3 deploy and configure the Service Option(s) selected by you;

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

8.2.5 on the date that BT has completed the activities in this Paragraph 8, subject to Paragraph 11.5, confirm to you that the Service is available for performance of any Acceptance Tests as set out in Paragraph 9.2.

8.3 **During Operation**

On and from the Service Start Date, BT:

8.3.1 will, for a period of five Business Days after the Service Start Date, implement any minor 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 6.4.4 and may be scheduled for implementation following this five Business Day period;

8.3.2 will maintain any relevant Customer Portal and server to provide you with online access to a range of functions including performance reports and placing CSP change requests in accordance with Paragraph 6.4;

8.3.3 may carry out Planned Maintenance from time to time and will endeavour to inform you at least five Business Days before any Planned Maintenance on the BT Equipment. However, you agree that BT may inform you with less notice than normal where emergency Planned Maintenance is required;

8.3.4 may, in the event of a security breach affecting the Service, require you to change any or all of your passwords. BT does not guarantee the security of the Service against unauthorised or unlawful access or use;

8.3.5 will, if you select either the BT Owned, Customer Owned or BT Takeover Service 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 your Site, for the purpose of Service monitoring and management;

8.3.6 will, if you select any of BT Owned, Customer Owned or BT Takeover Service delivery models, be responsible for ensuring software licences and any required support contracts are renewed for the term of this Contract. Unless you give BT Notice of an intention to terminate in accordance with Paragraph 6.2.2, 12 weeks prior to the end of the Contract, BT will extend the software licences and any required support contracts for a further 12 months;

8.3.7 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;

8.3.8 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 you to allow further remote management and diagnostics capability;

8.3.9 will, if you select the security consultancy Service Option as set out in Paragraph 3.1.16, capture the necessary information in consultation with your Customer Contact and produce the CSP;

8.3.10 will continuously monitor your Security Appliances at regular intervals over the Internet or other agreed network connection;

8.3.11 will for any of the BT Owned, Customer Owned and BT Takeover Service delivery models provide 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 0800 to 1700 Monday to Friday in the relevant country;

8.3.12 will send you 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 your Nominated Representative of potential High and Critical CVSS. 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;

8.3.13 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 you that the Patch is available for installation and provide additional information, where available, to support you in deciding whether to install the Patch or not;

8.3.14 will, following your request to implement the Patch, agree an installation window with you and confirm to you when the Patch has been installed; and

8.3.15 will roll the Patch back upon your request in the event that you detect 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 you for additional reasonable Charges.

8.4 **The End of the Service**

On termination of the Service by either one of us, or expiry, BT will:

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

8.4.2 where requested in writing prior to the termination of this Contract, provide, where reasonably practical, configuration information relating to the Service provided at the Site(s) in a format that BT reasonably specifies, provided you have, at that time, paid all Charges outstanding at and resulting from termination (whether or not due at the date of termination). You will pay all reasonable expenses incurred by BT in providing this information; and

8.4.3 have the right to disconnect and remove any BT Equipment located at the Site(s).

9 YOUR OBLIGATIONS

9.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Service by BT, you will:

9.1.1 provide BT with the names and contact details of any individuals authorised to act on your behalf for Service management matters ("**Customer Contact**"), but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;

9.1.2 provide BT with any information reasonably required without undue delay;

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

9.1.4 complete any preparation activities that BT may request to enable you to receive the Services promptly and in accordance with any reasonable timescales;

9.1.5 notify BT in writing of any health and safety rules and regulations and security requirements that apply at a Site;

9.1.6 in jurisdictions where an employer (or any other person who receives the Service) is legally required to make such disclosure to its employees or Users:

(a) inform your employees and users that as part of the Service being delivered by BT, BT may monitor and report to you the use of any targeted applications by your employees or Users; and

(b) ensure that your employees and users have consented or will be deemed to have consented to such monitoring and reporting (if such consent is legally required), agree that BT will not be liable for any failure by you to comply with this obligation and indemnify BT from and against any Claims or action brought by your employees or Users against BT arising out of the delivery of Services by BT;

9.1.7 ensure that the LAN protocols and applications you use will be compatible with the Service;

9.1.8 if you have not paid for Security Policy Production, submit a CSP that meets the requirements and specifications advised by BT at least 28 Business Days before the Customer Committed Date, including specifications that cover your 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 you at least ten Business Days before the Customer Committed Date;

9.1.9 retain responsibility for the CSP;

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

9.1.11 ensure that your MPLS/Internet access circuit bandwidth is sufficient to meet your requirements and the requirement for in-band management access from BT;

9.1.12 manage, and provide BT with accurate details of your internal IP address design;

9.1.13 register any required Internet domain names using legitimate addresses which are public, registered and routed to your Site;

9.1.14 modify your network routing to ensure appropriate traffic is directed to the Security Appliance. You acknowledge 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;

9.1.15 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;

9.1.16 obtain and provide in-life support for any Software running on your end user devices;

9.1.17 where necessary, provide and manage physical or virtual servers on your Site to a specification that BT agrees to run any Software that BT provides;

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

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

9.1.19 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;

9.1.20 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, not act to miss-use the Service as provided by BT to contravene or circumvent these laws. BT may treat any contravention of these laws as a material breach and:

(a) suspend the Service and BT may refuse to restore Service until BT receives an acceptable assurance from you that there will be no further contravention; or
(b) terminate the Service upon Notice in accordance with Clause 25 of the General Terms;

9.1.21 prepare and maintain the Site for the installation of BT Equipment and Customer Equipment and supply of the Service, including:

(a) providing a suitable and safe operational environment for any BT Equipment or Customer Equipment including all necessary trunking, conduits, cable trays, and telecommunications connection points in accordance with BT's reasonable instructions and in accordance with applicable installation standards;
(b) taking up or removing any fitted or fixed floor coverings, ceiling tiles and partition covers or providing any openings in buildings required to connect BT Equipment or Customer Equipment to appropriate telecommunications facilities in time to allow BT to undertake any necessary installation or maintenance Services;
(c) carrying out after installation any work that may be required to make good any cosmetic damage caused during the installation or maintenance Services;
(d) providing a secure, continuous power supply at the Site for the operation and maintenance of the Service and BT Equipment or Customer Equipment at such points and with such connections as BT specifies. In order to mitigate any Service interruption resulting from failure in the principal power supply, you will provide back-up power with sufficient capacity to conform to the standby requirements of the applicable British standards;
(e) providing internal cabling between the BT Equipment and any Customer Equipment, as appropriate; and
(f) complying with the Site Planning Guide.

9.1.22 in relation to BT Equipment:

(a) keep the BT Equipment safe and without risk to health;
(b) not use the BT Equipment, or allow it to be used, other than in accordance with any instructions BT may give and for the purpose for which it is designed;
(c) not move the BT Equipment or any part of it from the Site without BT's prior written consent and you will pay BT's costs and expenses reasonably incurred as a result of such move or relocation;

(d) not make any alterations, modifications, reconfigurations or attachments to the BT Equipment without BT's prior written consent. If BT gives BT's consent, any alterations, modifications, reconfigurations or attachments will become part of the BT Equipment;

(e) not sell, charge, assign, transfer or dispose of or part with possession of the BT Equipment or any part of it;

(f) not allow any lien, encumbrance or security interest over the BT Equipment, nor pledge the credit of BT for the repair of the BT Equipment or otherwise;

(g) not claim to be owner of the BT Equipment and ensure that the owner of the Site will not claim ownership of the BT Equipment, even if the BT Equipment is fixed to the Site;

(h) obtain appropriate insurance against any damage to or theft or loss of the BT Equipment;

(i) indemnify BT against all claims and proceedings arising from your use of the BT Equipment or if the BT Equipment is damaged, stolen or lost. You will keep BT informed of anything which may affect BT's rights, or involve BT in any proceedings, loss or liability; and

(j) if there is a threatened seizure of the BT Equipment, or Clause 18.3 of the General Terms applies to you, immediately notify BT and BT may take action to repossess the BT Equipment. You will also notify interested third parties that BT owns the BT Equipment;

9.1.23 identify and provide the name and contact details for a Nominated Representative responsible for liaising with BT regarding the Vulnerability Notification and Patching Service Option; and

9.1.24 advise BT if the Nominated Representative changes and ensure that BT has the current details of the Nominated Representative;

9.1.25 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 your 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.

9.2 **Acceptance Tests**

9.2.1 After receiving Notice from BT under Paragraph 8.2.5, you will promptly carry out the Acceptance Tests for the Service. The Service will be deemed to have been accepted if you have not:

(a) carried out the Acceptance Tests and confirmed acceptance in writing; or

(b) notified BT in writing that the Service has not passed the Acceptance Tests,

within five Business Days following notification under Paragraph 8.2.5.

9.2.2 Subject to Paragraph 9.2.3, the Service Start Date will be the earlier of the following:

(a) the date that you confirm acceptance of the Service in writing under Paragraph 9.2.1(a); or

(b) the date of notification under Paragraph 8.2.5.

9.2.3 In the event that the Acceptance Tests are not passed, BT will remedy the non-conformance without undue delay and notify you that BT has remedied the non-conformance, and inform you of the Service Start Date. Where the non-conformance is outside the scope of the Service, or due to delays or inaccuracies in information provided by you to BT, including the requirements of the CSP or the provisions of Paragraph 7.1, BT may apply additional Charges to remedy the non-conformances.

9.3 **Service Operation**

On and from the Service Start Date, you:

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

9.3.2 will ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and will be available for all subsequent Incident management communications;

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

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

9.3.5 will ensure that any Customer Equipment that is connected to the Service or that you use, directly or indirectly, in relation to the Service is:

(a) connected and used in accordance with any instructions, standards and safety and security procedures applicable to the use of that Customer Equipment;
(b) technically compatible with the Service and will not harm or damage BT Equipment, the BT Network, or any of BT's supplier's or subcontractor's network or equipment;
(c) approved and used in accordance with relevant instructions and Applicable Law; and
(d) adequately protected against viruses and other breaches of security;

9.3.6 will immediately disconnect any Customer Equipment, or advise BT to do so at your expense, if Customer Equipment does not meet any relevant instructions, standards or Applicable Law;

9.3.7 will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Service, including the Customer Portal;

9.3.8 will maintain a list of current Users and immediately terminate access for any person who ceases to be an authorised User;

9.3.9 will 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) inform BT immediately if a user 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;
(b) take all reasonable steps to prevent unauthorised access to the Service; and
(c) satisfy BT's security checks if a password is lost or forgotten;

9.3.10 will, if BT requests you to do so and in order to ensure the security or integrity of the Service, change any or all passwords or other systems administration information used in connection with the Service;

9.3.11 will comply with the provisions of any Software licences provided with or as part of the Service;

9.3.12 will, where you have selected the BT Owned, Customer Owned or BT Takeover Service 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;

9.3.13 will request, if applicable, up to five login/password combinations for access to a Customer Portal for use by you or your agents. You may assign one login combination to BT's personnel. You are responsible for your agents' use of these IDs;

9.3.14 will, for the BT Takeover Service 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; and

9.3.15 agree that:

(a) BT may share Customer information (including Personal Data) with the supplier of BT Equipment or Customer Equipment as may be necessary for the provision and management of the Service. Depending on the Service(s) provided, Customer information may be automatically sent from Security Appliances or Software to cloud-based infrastructure operated by the supplier;
(b) Processing of Customer information (including Personal Data) will be subject to the relevant supplier's EULA (where applicable) and privacy policy as may be amended or supplemented from time to time by the supplier. You agree that BT will not be liable for any claim arising out of or in connection with any failure by the supplier to comply with the supplier's EULA (where applicable) and privacy policy and any claims will be made directly by you against the supplier;
(c) BT will not be liable for failure to or delay in supplying the Service if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost;
(d) BT will provide the Service to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the Service:

(i) will be performed error-free or uninterrupted or that BT will correct all errors in the Service;
(ii) the Service will operate in combination with your content or applications or with any other software, hardware, systems or data;
(iii) the Service, including any products, information or other material you obtain under or in connection with this Contract, will meet your requirements; and
(iv) the Service will detect or block all malicious threats;

(e) BT will not be liable in the event that Software updates from the supplier used to identify and control your 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;

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

(g) customer information may be transferred or stored outside the European Economic Area or the country where you and your Users are located in order to carry out the Service and BT's other obligations under this Contract; and

(h) you 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 you in connection with the Service, or any actions taken by BT at your direction.

9.4 **The End of the Service**

On termination of the Service by either one of us, or expiry you will:

9.4.1 provide BT with all reasonable assistance necessary to remove BT Equipment from the Sites;

9.4.2 disconnect any Customer Equipment from BT Equipment located at the Sites;

9.4.3 not dispose of or use BT Equipment, other than in accordance with BT's written instructions or authorisation;

9.4.4 arrange for any BT Equipment, including software, located at the Sites to be returned to BT; and

9.4.5 be liable for any reasonable costs of recovery that BT incurs in recovering the BT Equipment.

10 NOTIFICATION OF INCIDENTS

Where you become aware of an Incident:

10.1 the Customer Contact will report it to BT's Service Desk;

10.2 BT will give you a unique reference number for the Incident ("**Ticket**");

10.3 BT will inform you when BT believes the Incident is cleared, and will close the Ticket when:

10.3.1 you confirm that the Incident is cleared within 24 hours of being informed; or

10.3.2 BT has attempted unsuccessfully to contact you, in the way agreed between both of us, in relation to the Incident and you have not responded within 24 hours of BT's attempt to contact you.

10.4 If you confirm that the Incident is not cleared within 24 hours of being informed, the Ticket will remain open and BT will continue to work to resolve the Incident.

10.5 Where BT becomes aware of an Incident, Paragraphs 10.2, 10.3 and 10.4will apply.

10.6 BT will keep you informed throughout the course of the Incident resolution at regular intervals. Updates may be provided by telephone, email or through your BT My Account.

11 INVOICING

11.1 BT will invoice you for the Charges for the Service as set out in Paragraph 11.2 in the amounts and currency specified in any Orders.

11.2 Unless stated otherwise in an applicable Order, BT will invoice you for:

11.2.1 Installation Charges, on the Service Start Date or monthly in arrears prior to the Service Start Date for any work carried out where the planned installation period is longer than one month;

11.2.2 the following components, depending on the options selected in 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	Charges relating to the supply and installation of Security Appliances provided on a rental basis	Different charges apply according to location and to different appliances, depending on vendor and model.

Pricing Component	One-time Charge	Recurring Charge	Notes
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 your IP addresses or Users
Service Provision	Charges relating to project management and Service commissioning	N/A	Also applies to in-life changes to the Service.
Service Management	Set-up	Monthly Management	Covers provision and ongoing delivery of Service Options, including Out of Band management capability, Incident management and proactive service monitoring.
Configuration Management	Per Occasion (Pay as You Go)	Monthly Management (Unlimited changes)	Covers implementation of CSP change requests.
Professional Services	Consultancy	N/A	Initial (optional) capture of CSP. Ad hoc consultancy as requested (charged on a per day basis).
Service De-Installation	Service De-Commissioning	N/A	Covers disconnection and removal of BT Equipment from your Site at end of Contract.

11.2.3 any Termination Charges incurred are payable in accordance with Paragraph 12 upon termination of the relevant Service.

11.3 BT may invoice you for any of the following Charges in addition to those set out in the Order:

11.3.1 Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is outside the Service Management Boundary or where (in the case of Service Wrap Only) the cause of the Incident was found to be as a result of faulty Customer Equipment;

11.3.2 Charges for restoring Service if the Service has been suspended in accordance with Clause 10.1.2 of the General Terms;

11.3.3 Charges for cancelling the Service in accordance with Clause 16 of the General Terms;

11.3.4 Charges for expediting provision of the Service at your request after you have been informed of the Customer Committed Date;

11.3.5 Charges for the refresh or upgrade of appliances or applications if required by you, unless the refresh or upgrade is operationally necessary to enable BT to continue to provide the Service. This does not apply to patching of applications or changes to the CSP. 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 will be charged to you;

11.3.6 Charges incurred due to inaccuracies in information provided by you to BT, including the requirements of the CSP or the provisions of Paragraph 7.1; and

11.3.7 any other Charges set out in any applicable Order or the BT Price List or otherwise agreed between both of us.

11.4 Subject to Paragraph 11.2.1, the invoicing start date for the Service is the Service Start Date.

11.5 BT will usually install and configure BT Equipment or Customer Equipment (where relevant) on the same day. If you require BT to delay configuration once the BT Equipment or Customer Equipment has been installed, BT may commence invoicing for the BT Equipment or Customer Equipment from the date of installation. If configuration is delayed for more than 30 days at your request, BT may commence invoicing for the Service.

12 CHARGES AT THE END OF THE CONTRACT

12.1 If you exercise your right under Clause 17 of the General Terms to terminate the Contract or any Service, for convenience, you will pay BT:

12.1.1 all outstanding Charges for Services rendered;

12.1.2 any other Charges set out in the Order;

12.1.3 any additional Charges that BT has to pay a supplier as a result of early termination of the Service;

12.1.4 any remaining Charges outstanding with regard to BT Equipment;

12.1.5 De-installation Charges where appropriate; and

12.1.6 any unrecovered third party charges arising from cancellation of third party contracts.

12.2 In addition to the Charges set out at Paragraph 12.1 above, if you terminate during the Minimum Period of Service you will pay BT:

12.2.1 for any parts of the Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to:

(a) 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service; and

(b) 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service; and

(c) any waived Installation Charges; and

12.2.2 for any parts of the Service that were terminated after the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

13 SERVICE AMENDMENT

13.1 You may request, by giving BT Notice, a change to:

13.1.1 an Order for the Service (or part of an Order) at any time before the applicable Service Start Date, as set out in Paragraph 8.1.4; or

13.1.2 the Service at any time after the Service Start Date.

13.2 If you exercise your right under Paragraph 13.1, and except where a change results from BT's failure to comply with BT's obligations under the Contract, BT will, within a reasonable time, provide you with a written estimate, including:

13.2.1 the likely time required to deliver the changed Service; and

13.2.2 any changes to the Charges due to the changed Service.

13.3 BT has no obligation to proceed with any change that you request under Paragraph 13.1, unless and until we have both agreed in writing on the necessary changes to the Charges, implementation timetable and any other relevant terms of the Contract to take account of the change.

13.4 If BT changes a Service prior to the Service Start Date because you have given BT incomplete or inaccurate information, BT may apply additional reasonable one-time or Recurring Charges.

14 IP ADDRESSES AND DOMAIN NAMES

14.1 Except for IP Addresses expressly registered in your name, all IP Addresses and Domain Names made available with the Service will at all times remain BT's property or the property of BT's suppliers and will be non-transferable. All of your rights to use such IP Addresses or Domain Names will stop on termination or expiration of the Service.

14.2 BT cannot ensure that any requested Domain Name will be available from or approved for use by the Internet Registration Authorities and BT has no liability for any failure in the Domain Name registration, transfer or renewal process.

14.3 You will not use IP addresses that you do not own or that are incorrectly specified and you will be responsible for the use of IP addresses within your network. BT may apply charges for dealing with changes or Incidents that occur as a result of incorrect / illegal IP addressing schemes.

14.4 You warrant that you are the owner of, or are authorised by the owner of the trade mark or name that you wish to use as a Domain Name, and that such Domain Name will not infringe the rights of any person in a corresponding trade mark or name.

14.5 You are responsible for all fees associated with registration and maintenance of your Domain Name, and will reimburse BT for any and all fees that BT pays to any Internet Registration Authorities, and thereafter be responsible for paying such fees directly to the relevant Internet Registration Authorities.

15 BT EQUIPMENT

15.1 BT Equipment will remain BT's property at all times and risk in BT Equipment will pass to you upon delivery, whether or not the BT Equipment has been installed.

15.2 You will be liable to BT for any loss of or damage to BT Equipment, except where the loss or damage is a result of fair wear and tear or caused by BT.

16 WEEE DIRECTIVE

16.1 Where required under the terms of Article 13 of the Waste Electrical and Electronic Equipment Directive 2012 ("**WEEE Directive**"), you will be responsible for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Contract that has become waste electrical and electronic equipment ("**WEEE**").

16.2 Each of us acknowledge that for the purposes of Article 13 this Paragraph 16 is an agreement stipulating other financing arrangements for the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE.

16.3 You will be responsible for any information recording or reporting obligations imposed by the WEEE Directive.

16.4 You will indemnify BT against any claims or legal proceedings that are brought or threatened against BT by a third party which would not have been caused or made had you fulfilled your express or implied obligations under this Paragraph 16 or in connection with the WEEE Directive.

16.5 BT will notify you of any such claims or proceedings and keep you informed as to the progress of such claims or proceedings.

Part C – Service Levels

17 ON TIME DELIVERY

17.1 **On Time Delivery Service Level**

17.1.1 BT will deliver the Service on or before the Customer Committed Date (the "**On Time Delivery Service Level**").

17.2 **On Time Delivery Service Credits**

17.2.1 If BT does not meet the On Time Delivery Service Level, you may claim On Time Delivery Service Credits for each day after the Customer Committed Date until the Service is delivered at the Site, as set out in this Paragraph 17.2.

17.2.2 You may claim On Time Delivery Service Credits by reporting any failure to meet the On Time Delivery Service Level to the Service Desk in accordance with Paragraph 10.

17.2.3 On Time Delivery Service Credits are available up to a maximum amount equal to 100 per cent of the monthly Recurring Charge for the affected Site or Circuit.

17.2.4 If both of us have agreed a revised Customer Committed Date in writing, or if BT exercises BT's right to revise the Customer Committed Date as set out in Paragraph 17.3.1, the calculation of any On Time Delivery Service Credits will be made by reference to the revised Customer Committed Date.

17.3 **Exceptions**

17.3.1 If you request a change to the Service or any part of the Service, including any BT Equipment or Customer Equipment or any IP Address location, or delay the completion of your obligations as set out in Paragraph 9, then BT may change the Customer Committed Date to accommodate that change or delay.

17.3.2 The On-Time Delivery Service Level does not apply to upgrades or changes to the Services, unless these require the installation of new components and have an agreed delivery date, in which case the Customer Committed Date will be that agreed delivery date.

17.3.3 BT may expedite delivery of the Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

18 SERVICE AVAILABILITY

18.1 **Availability Service Level**

18.1.1 From the Service Start Date, BT will provide the Service with a target availability corresponding to the agreed SLA Category for the Service as set out in the table in Paragraph 18.2.2 below (the "**Availability Service Level**").

18.1.2 You may request Availability Service Credits for Qualifying Incidents at either:

(a) the Standard Availability Service Credit Rate, as set out in Paragraph 18.3.5; or

(b) as applicable, the Elevated Availability Service Credit Rate, as set out in Paragraph 18.3.6.

18.2 **SLA Categories**

18.2.1 The SLA Categories depend on a number of factors, including:

(a) any applications you deploy and any CSP you implement;

(b) the broader network and server environment including any resilient elements; and

(c) the physical location of the Security Appliances and availability of on-site field support.

18.2.2 The following table sets out the Availability Annual Targets, the Maximum Annual Availability Downtime, the Maximum Monthly Availability Downtime, the Standard Availability Service Credit Rate, the Elevated Availability Service Credit Rate and the Service Credit Interval for each SLA Category:

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Downtime	Standard Availability Service Credit Rate	Elevated Availability Service Credit Rate	Service Credit Interval
Cat A++	≥ 99.999%	5 minutes	0 minutes	4%	8%	5 min
Cat A+	≥ 99.99%	1 hour	0 minutes	4%	8%	15 min
Cat A1	≥ 99.97%	3 hours	0 minutes	4%	8%	1 hour
Cat A	≥ 99.95%	4 hours	0 minutes	4%	8%	1 hour
Cat B	≥ 99.90%	8 hours	1 hour	4%	8%	1 hour

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Downtime	Standard Availability Service Credit Rate	Elevated Availability Service Credit Rate	Service Credit Interval
Cat C	≥ 99.85%	13 hours	3 hours	4%	4%	1 hour
Cat D	≥ 99.80%	17 hours	5 hours	4%	4%	1 hour
Cat E	≥ 99.70%	26 hours	7 hours	4%	4%	1 hour
Cat F	≥ 99.50%	43 hours	9 hours	4%	4%	1 hour
Cat G	≥ 99.00%	87 hours	11 hours	4%	4%	1 hour
Cat H	≥ 98.00%	175 hours	13 hours	4%	4%	1 hour
Cat I	≥ 97.00%	262 hours	15 hours	4%	4%	1 hour

18.3 **Availability Service Credits**

18.3.1 If a Qualifying Incident occurs, BT will measure and record the Availability Downtime for the Site starting from when you report or BT gives you notice of a Qualifying Incident, and ending when BT closes the Incident in accordance with Paragraph 10.3.

18.3.2 BT will measure the Availability Downtime in units of full minutes during the Local Contracted Business Hours for Access Line Incidents, and during the Contracted Maintenance Hours for BT Equipment Incidents.

18.3.3 Following the measurement taken in accordance with Paragraph 18.3.1 and Paragraph 18.3.2, BT will calculate the cumulative Availability Downtime for the calendar month(s) in which the Qualifying Incident occurred (the "**Cumulative Monthly Availability Downtime**") and for the previous 12 consecutive calendar months (the "**Cumulative Annual Availability Downtime**"), but in the event that the Site has been installed for less than 12 consecutive months.

18.3.4 In the event a Site has been installed for less than 12 consecutive months, BT will apply an assumed Cumulative Annual Availability Downtime for the previous 12 consecutive months for that Site or Circuit using the Availability Downtime data recorded to date.

18.3.5 If the Cumulative Monthly Availability Downtime of the Site exceeds the Maximum Monthly Availability Downtime, you may request Availability Service Credits for each stated Service Credit Interval above the Maximum Monthly Availability Downtime.

18.3.6 If the Cumulative Annual Availability Downtime of the Site or Circuit exceeds the Maximum Annual Availability Downtime, you may request Availability Service Credits for all further Qualifying Incidents at the Elevated Availability Service Credit Rate for each started Service Credit Interval above the Maximum Annual Availability Downtime up to and until the Cumulative Annual Availability Downtime by Service is less than the Maximum Annual Availability Downtime.

18.3.7 Availability Service Credits are available up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.

19 RESILIENCY RESTORATION

19.1 **Resiliency Restoration Service Level**

Where you have purchased a Resilient Service and experience loss of Service on any Resilient Component (which does not amount to a Severity Level 1 Incident), BT aims to restore Service to the affected Resilient Components within one Business Day of you reporting the Incident, or BT detecting the Incident, ("**Resiliency Restoration Service Level**"). The Resiliency Restoration Service Level will not apply where there is a Qualifying Incident (in which case, the Availability Service Level will apply, in accordance with Paragraph 18).

19.2 **Resiliency Restoration Service Credits**

19.2.1 If the affected Resilient Components are not restored within one Business Day, you may request a Resilience Restoration Service Credit for each commenced hour in excess of the Resiliency Restoration Service Level.

19.2.2 This Service Credit only applies where the Resilient Component is covered by an on-site maintenance agreement of next Business Day or shorter.

20 REQUESTS FOR SERVICE CREDITS

20.1 You may request applicable Service Credits within 28 days of the end of the calendar month in which an Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 20.1 will constitute a waiver of any claim for Service Credits for that calendar month.

20.2 Upon receipt of a valid request for Service Credits in accordance with Paragraph 20.1;

20.2.1 BT will issue you with the applicable Service Credits by deducting those Service Credits from your invoice within two billing cycles of the request being received; and

20.2.2 following expiry or termination of the Contract where no further invoices are due to be issued by BT, BT will pay you the Service Credits in a reasonable period of time.

20.3 All Service Levels and Service Credits will be calculated in accordance with information recorded by, or on behalf of, BT.

20.4 The Service Levels under this Schedule will not apply:

20.4.1 in the event that Clause 8 of the General Terms applies;

20.4.2 during any trial period of the Service;

20.4.3 to failures due to any Force Majeure Event;

20.4.4 to uptime of the cloud-based firewall as set out in Paragraph 3.1.10;

20.4.5 if you cause a delay or do not provide any requested information in accordance with any reasonable timescales BT tells you about; or

20.4.6 to any Incident not reported in accordance with Paragraph 10 above.

20.5 **CSP Change Request Delivery Time Targets**

20.5.1 Targets apply to Urgent Changes and Standard Changes.

20.5.2 If you submit a change with more than five lines of changes, the target times below will not apply.

20.5.3 The completion time for the change will be notified to you by BT.

20.5.4 The response time for the changes is listed below:

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

20.5.5 Service Credits do not apply to CSP change requests and to the Vulnerability Notification and Patching Service Option.

Part D – Defined Terms

21 DEFINED TERMS

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

"**Acceptance Tests**" means those objective tests conducted by you, which, when passed confirm that you accept the Service and that the Service is ready for use save for any minor non-conformities, which will be resolved as an Incident as set out in Paragraph 10.

"**BT Managed Firewall Security**" has the meaning given to it at Paragraph 1.2.1.

"**BT Managed Web Security**" has the meaning given to it at Paragraph 1.2.2.

"**Annual 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.

"**Availability**" means the period of time when the Service is functioning.

"**Availability Downtime**" means the period of time during which a Qualifying Incident exists as measured by BT in accordance with Paragraph 18.3.1.

"**Availability Service Credit**" means the Service Credit calculated at the Standard Availability Service Credit Rate or at the Elevated Availability Service Credit Rate as applicable.

"**Availability Service Level**" has the meaning given in Paragraph 18.1.1.

"**BT Network**" means the communications network owned or leased by BT and used to provide the Service.

"**BT Owned**" has the meaning given to in Paragraph 2.1.3(a).

"**BT Takeover**" has the meaning given in Paragraph 2.1.3(c).

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted, and that is provided as part of the Service.

"**Contracted Maintenance Hours**" means the times during which BT will provide maintenance for BT Equipment, which will be Business Hours unless specified otherwise in the Order.

"**Critical CVSS score**" means a CVSS score range from 9.0 to 10.0.

"**Cumulative Annual Availability Downtime**" has the meaning given in Paragraph 18.3.3.

"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 18.3.3.

"**Customer Committed Date**" has the meaning given in Paragraph 8.1.3.

"**Customer Contact**" has the meaning given in Paragraph 9.1.1.

"**Customer Equipment**" means any equipment (including any purchased and owned by the customer) and any software, other than BT Equipment, used by you in connection with a Service.

"**Customer Portal**" means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the Service.

"**Customer Owned**" has the meaning given in Paragraph 2.1.3(b).

"**CSP**" means your customer security policy containing the security rules, set and owned by you, that are applied to the BT Equipment or Customer Equipment and determine the operation of the Service.

"**CVSS**" means Common Vulnerability Scoring System v3.0.

"**De-installation Charges**" means the charges payable by you on de-installation of the Service that will be equal to the then current rates for Installation Charges on the date of de-installation.

"**DMZ**" means de-militarised zone.

"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.

"**Elevated Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 18.2.2 for the relevant SLA Category.

"**Emergency Change**" means a change that requires immediate attention from SOC to address a live, service impacting issue that you are experiencing. Emergency change should be used only as a last resort.

"**Enabling Service**" has the meaning given in Paragraph 5.1.

"**Ethernet**" means a family of computer networking technologies for LANs.

"**EULA**" has the meaning given to it in Paragraph 6.3.

"**Fixed Annual Price**" means the price that is agreed with you at the start of the year and charged either monthly or quarterly as set out in the Order.

"**High CVSS score**" means a CVSS score range from 7.0 to 8.9.

"**HTTPS**" means a communication protocol for secure communication over a computer network.

"**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 an unplanned interruption to, or a reduction in the quality of, the Service or particular element of the Service.
"**Installation Charges**" means those Charges set out in the Order in relation to installation of the Service or any Customer Equipment or BT Equipment as applicable.
"**Integrated Services Digital Network**" or "**ISDN**" means a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the PSTN.
"**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.
"**IM**" means instant messaging communications.
"**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).
"**Local Contracted Business Hours**" means the times during which maintenance of any Access Line is provided, which will be Business Hours unless specified otherwise in the Order.
"Managed Service" means a managed voice or/and data telecommunications service. Management services are provided as an overlay to the following services to provide a fully managed solution:

(a) Wide Area Network (WAN);
(b) Local Area Network (LAN);
(c) Unified Communications (UC).

"**Managed Service Schedule to the General Terms**" means a Service Schedule for Managed Services that can be found at https://www.globalservices.bt.com/en/terms-and-conditions.
"**Managed Service from BT**" means a managed voice or/and data telecommunications service. Management services are provided as an overlay to the following services to provide a fully managed solution:

(a) Wide Area Network (WAN);
(b) Local Area Network (LAN);
(c) IP Telephony (IPT);
(d) Security;
(e) Applications such as Microsoft Services and AAI.

"**Managed Service from BT Schedule to the General Terms**" means a Service Schedule for Managed Service from BT that can be found at https://www.globalservices.bt.com/en/terms-and-conditions/managed-service-from-bt-terms-and-conditions.
"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 18.2.2 for the relevant SLA Category.
"**Maximum Monthly Availability Downtime**" has the meaning given in the table at Paragraph 18.2.2 for the relevant SLA Category.
"**Minimum Period of Service**" means a period of three years beginning on the Service Start Date, unless otherwise set out in an Order.
"**Multi-Protocol Label Switching**" or "**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 your organisation nominated to be the point of contact for Vulnerability notifications.
"**On Time Delivery Service Credits**" means four per cent of the Recurring Charges for the applicable Site, per day.
"**On Time Delivery Service Level**" has the meaning given in Paragraph 17.1.
"**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.
"**PSTN**" means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.

"**Qualifying Incident**" means a Severity 1 Level Incident, except where any of the following events have occurred:

(a) the Service has been modified or altered in any way by you, or by BT in accordance with your instructions;
(b) Planned Maintenance;
(c) you have performed any network configurations that BT did not approve;
(d) an Incident has been reported and BT cannot confirm that an Incident exists after performing tests; or
(e) you requested BT to test the Service at a time when no Incident has been detected or reported.

"**Recurring Charges**" means the Charges for the Service or applicable part of the Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in the Order.

"**Resiliency Restoration Service Credit**" means one per cent of the total monthly Recurring Charges for the Resilient Service up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.

"**Resiliency Restoration Service Level**" has the meaning given in Paragraph 19.1.

"**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 you select in accordance with Paragraph 2.1.3) used to apply the CSP.

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

"**Service Credit**" means each of the Availability Service Credit, the On Time Service Delivery Service Credit and the Resiliency Restoration Service Credit.

"**Service Credit Interval**" means as set out in the table at Paragraph 18.2.2 for the relevant SLA Category.

"**Service Desk**" has the meaning given in Paragraph 8.1.1.

"**Service Level**" means each of the On Time Delivery Service Level, the Availability Service Level and the Resiliency Restoration Service Level.

"**Service Management Boundary**" has the meaning given in Paragraph 4.

"**Service Wrap Only**" has the meaning given in Paragraph 2.1.3(d).

"**Severity Level 1 Incident**" means an Incident that cannot be circumvented and that constitutes a complete loss of Service at the Site or Circuit and in respect of a Resilient Service, excluding any loss of service of a Resilient Component where you still have access to the Service through the other back-up Resilient Component.

"**Site**" means a location at which the Service is provided.

"**Site Planning Guide**" means a guide provided by BT to you detailing the hardware specification, including environmental, physical and electrical details of any BT Equipment provided to you with the Service.

"**SLA Category**" means the category, as set out in the Order which, in accordance with the table set out at Paragraph 18.2.2, specifies the following in relation to the Service, Site or Circuit:

(a) Availability Annual Target;
(b) Maximum Annual Availability Downtime;
(c) Maximum Monthly Availability Downtime;
(d) Standard Availability Service Credit Rate;
(e) Elevated Availability Service Credit Rate; and
(f) Service Credit Interval.

"**SOC**" means Security Operations Centre.

"**SSL**" means secure sockets layer.

"**Standard Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 18.2.2 for the relevant SLA Category.

"**Standard Change**" means upgrades and modifications resulting from planned developments and security improvements.

"**Ticket**" has the meaning given in Paragraph 10.2.

"**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. Urgent changes are always chargeable.

"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.

"**Vulnerability**" means a Software susceptibility that may be exploitable by an attacker.
"**WEEE**" has the meaning given in Paragraph 16.1.
"**WEEE Directive**" has the meaning given in Paragraph 16.1.
"**Wide Area Network**" or "**WAN**" means the infrastructure that enables the transmission of data between Sites.