BT Managed Security Services
Service 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) XXXXXXXXXX Title: XXXXXXXXXX	Paul Rhodes NIF of representative (ID Number): X0.688.132-H Title: Legal representative

1 DEFINITIONS AND ABBREVIATIONS

In addition to the defined terms in the General Terms and Conditions, capitalised terms in this Schedule will have the meanings below (and in the case of conflict between these defined terms and the defined terms in the General Terms and Conditions or the Associated Services Annexes, these defined terms will take precedence for the purposes of this Schedule).

"**Alert Logs**" means logs that track alert events (e.g. anomaly detection).
"Annex" means any annex to the Schedule for an Associated that describes a Service or sets out the specific terms that apply to it.
"**Associated Services**" means the BT products and services that the Customer can use with the BT Managed Security Service and that are set out in the Order.
"**Audit Logs**" means logs that track changes (e.g. firewall rule changes) and access (authentication/authorisation) attempts.
"**BT Equipment**" means any equipment and any related Software that BT owns or that is licensed to BT and that BT uses to provide the BT Managed Security Service or the Associated Services.
"**BT Managed Security Service**" has the meaning given in this Schedule.
"**BT Network**" means the communications network owned or leased by BT and used to provide a BT Managed Security Service or an Associated Service.
"**BT Personnel**" means all those employees of BT who are engaged in the provision of the BT Managed Security Service or Associated Services (or relevant part of the BT Managed Security Service or Associated Services) from time to time.
"**BT Project Manager**" means the project manager BT appoints to liaise with the Customer on Initial Setup matters as set out in this Schedule.
"BT Security Portal" means one or more webpages made available to the Customer by BT to provide for one or more specific functions in relation to the BT Managed Security Service or Associated Services.
"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.
"**Complex Change**" means a change that is not a Simple Change as set out in Paragraph 14.1.
"**Continuous Improvement**" means the continuous improvement phase of the BT Managed Security Service as set out in Paragraph 12 and 13.
"**Controlled Deployment**" means the controlled deployment phase of the BT Managed Security Service as set out in Paragraph 5.
"**Controlled Deployment CSP Optimisation**" means the fine tuning of the Customer's CSP(s), conducted by the Customer or in respect of Foundation Plus or Premium only both Parties jointly as set out in Paragraph 5.
"**Controlled Deployment CSP Optimisation Period**" means in respect of:

(a) Foundation, 48 hours after receiving notice from BT;
(b) Foundation Plus, up to 30 Business Days after receiving notice from BT; and
(c) Premium, up to 30 Business Days after receiving notice from BT.

"**Critical CVSS Score**" means a CVSS score range from 9.0 to 10.0.
"**CSP Change Management Process**" means the process in relation to changes to the CSP(s) as set out in this Schedule.
"**Customer Committed Date**" means for the purpose of the On-Time Delivery Service Level as set out in Paragraph 19 of this Schedule; the date provided by BT on which delivery of an Associated Service including the ordered the BT Managed Security Service (or each part thereof, including to each Site) is due to start.

"**Customer Equipment**" means any equipment (including any purchased and owned by the Customer) and any software, other than BT Equipment, used by the Customer in connection with an Associated Service.
"**Customer Handbook**" means a document provided to the Customer upon completion of the Initial Setup phase to provide you with information relevant to the BT Managed Security Service and Graded Service Tier purchased. The Customer Handbook is not a contractual document.
"**Customer Security Policy**" or "**CSP**" means the Customer's security policy containing the security rules, set and owned by the Customer, that are applied to the applicable Associated Service and determine the operation of the applicable Associated Service.
"**CVSS**" means Common Vulnerability Scoring System v3.0.
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**Emergency Change**" means a highly critical, Simple Change means as set out in Paragraph 14.1.
"**Enabling Service**" means services that are necessary for an Associated Service to function as set out in the Associated Service Annex and the Customer will ensure that these services meet the minimum technical requirements that BT specifies.
"**EULA**" has the meaning given in Paragraph 17.3
"**Foundation**" means the Foundation Graded Service Tier as set out in this Schedule.
"**Foundation Plus**" means the Foundation Plus Graded Service Tier as set out in this Schedule.
"**Graded Service Tier**" is the term used to describe the level of management features for the BT Managed Security Service and is classified as either Foundation, Foundation Plus or Premium.
"**High CVSS Score**" means a CVSS score ranging from 7.0 to 8.9.
"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Managed Security Service or Associated Services or particular element of the BT Managed Security Service or Associated Services.
"**Initial Setup**" means the facilitation of the setup and delivery of the Associated Services as set out in Paragraph 4.
"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.
"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**Local Area Network**" or "**LAN**" means the infrastructure that enables the ability to transfer IP services within Site(s) (including data, voice and video conferencing services).
"Maintenance" means any work on the BT Network or BT Managed Security Services or Associated Services, including to maintain, repair or improve the performance of the BT Network or BT Managed Security Services or Associated Services.
"**Medium CVSS score**" means a CVSS score ranging from 5.0 to 6.9.
"**Minimum Period of Service**" means a period of 12 consecutive months beginning on the Operational Service Date, unless set out otherwise in the Annex for an Associated Service or the applicable Order.
"**Monitoring and Management**" means the monitoring and management phase of the BT Managed Security Service as set out in this Schedule.
"**On Time Delivery Service Level**" has the meaning given in Paragraph 19.
"**Operational Logs**" means logs that track activity (e.g. allow/deny on a firewall).
"**Operational Service Date**" means the date BT first makes a BT Managed Security Service and an Associated Service available to the Customer which will be the date of completion of the Initial Setup.
"**P1**" - "**P2**" - "**P3**" - "**P4**" and "**P5**" has the meaning given in the table at Paragraph 8.1.4.
"**Patch**" means vendor provided software intended to address a specific Vulnerability.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**Premium**" means the Premium Graded Service Tier as set out in this Schedule.
"**Professional Services**" means those services provided by BT which are labour related services.
"**Qualifying Incident**" means an Incident, resulting in a total loss of Service (both primary and any resilience/back-up) to a Site or Service; except if this was due to an excluded event as set out in this Schedule or the Annex of an Associated Service.
"**Reasonable Use Policy**" means a number of Simple Changes included in the Charges as further set out in Paragraph 14.1.10.
"**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 any applicable Order. This may include Charges relating to recurring licenses and third party support agreements.
"**Renewal Period**" means for each BT Managed Security Service, the initial 12 month period following the Minimum Period of Service, and each subsequent 12 month period, or any period as agreed by both Parties.

"**Resource**" means a physical resource such as CPU or RAM present on a Security Appliance utilised during the use of the Security Appliance and exhaustion of that Resource would cause an Incident in or degradation of the relevant Associated Service.
"**Security Appliance**" means the BT Equipment or Customer Equipment that BT manages on the Customer's behalf as part of the Associated Services used to apply the CSP(s). The Security Appliance may be physical or virtual.
"**Security Operations Centre**" or "**SOC**" means the BT team responsible for the Monitoring and Management of the Associated Services provided under the BT Managed Security Service.
"**Security Optimisation Manager**" means the security manager appointed by BT who will work with the Customer in respect of the activities as set out in Paragraphs 12.
"**Security Threat Intelligence**" or "**STI**" means the security threat intelligence service set out in Paragraph 6.
"Service" may either mean BT Managed Security Services, an Associated Service or the combination of both.
"Service Credit" means any remedy for failure by BT to meet a Service Level as set out in the Schedule.
"**Service Desk**" means the helpdesk that the Customer is able to contact to submit service requests, report Incidents and ask questions about the BT Managed Security Service or the Associated Services.
"**Service Level**" means the On Time Delivery Service Level set out in this Schedule and the Service Levels set out in the applicable Associated Service(s) Annex(es).
"**Service Management Boundary**" has the meaning given in Paragraph 18.
"**Service Target**" means any target that BT aims to meet as set out in this Schedule or an Associated Service Schedule or Annex.
"**Signature Updates**" means vendor specific updates that address the known counter measure to threats.
"**Simple Change**" means the Simple Changes as set out in Paragraph 14.1 and as further specified in the Annex for each Associated Service.
"**Site**" means a location at which the BT Managed Security Service or the Associated Service is provided.
"**Standard Change**" means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements as set out in Paragraph 14.1.
"**Target Implementation Time**" means the target implementation time from acceptance by BT of the Customer's CSP change request as set out in the table in Paragraph **Error! Reference source not found.**.
"**Target Restoration Time**" has the meaning given in the table at Paragraph 8.1.5 for the relevant priority level and Graded Service Tier.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Unified Threat Management**" or "**UTM**" means an approach to information security where a single hardware or software installation provides multiple security functions.
"**Urgent Change**" means a Simple Change as set out in Paragraph 14.1 requiring urgent 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.
"**User Guides**" means the documents that set out details on how the Customer:

(a) access the BT Security Portal;
(b) make changes to the CSP(s); and
(c) access reports.

"**Vulnerability**" means a software susceptibility that may be exploited by an attacker.
"**Vulnerability Management and Patching**" means the vulnerability management and patching of Security Appliances services set out in Paragraph 13.

2 SERVICE SUMMARY

2.1 BT Managed Security Service provides the Customer with a range of graded security management services which can be used in association with, and as an overlay to, Associated Services ("BT Managed Security Service").

2.2 This Schedule provides an overview of the available Graded Service Tiers which can be applicable to a specific Associated Service and the related applicable conditions in general. To which extend a Graded Service Tier apply on an Associated Service shall be set out in the specific Annex of such Associated Service and when ordering such Associated Service the Customer will select the required Graded Service Tier and the relevant features on the Order.

3 OVERVIEW OF POSSIBLE GRADED SERVICE TIERS

3.1 The applicable Graded Service Tiers which may be available for a specific Associated Services are set out in the table below:

	Foundation	Foundation Plus	Premium
Delivery - Initial Setup of the Associated Services			
Customer Security Policy			
Associated Services	Good practice standard policies	Customisable security policy	Customisable security policy
BT Project Manager assigned for Initial Setup	✗ Upgrade available as Service Option	✓ Named Upgrade available as Service Option	✓ Named & potential Site visit depending on location.
On Time Delivery Service Levels available	✗	✓	✓
Delivery - Controlled Deployment of the Associated Services			
Controlled Deployment CSP Optimisation Period commences on completion of Initial Setup			
Associated Services Controlled Deployment CSP Optimisation Period	Estimated time spend by BT: 48 hrs	Estimated time spend by BT: Up to 30 days	Estimated time spend by BT: Up to 30 days
BT support for CSP test and tune	✗	✓	✓
In Life - Monitoring and Management of the Associated Services			
Security Threat Intelligence - Threat Intelligence Bulletins and Reports	✓	✓	✓
Proactive Monitoring			
Monitor for impending issues that may affect the Associated Services	✓ Associated Services polling to check power and network connectivity, status testing, monitoring unauthorised access attempts	✓ Additionally to Foundation; monitoring of applications under Associated Services	✓ Additionally to Foundation Plus; password management and certificate expiry monitoring
Manage Service Incidents			
Service Desk 24x7x365	✓	✓	✓
Security Operations Centre (SOC)	BT selects appropriate SOC	BT selects appropriate SOC	The Customer may opt for a regional SOC when available
Service Desk language	English	English	As agreed with BT (English by default)
Signature Updates	BT will identify test and implement Signature Updates for Unified Threat Management functions of the Associated Services		
Log Capture			
Log availability on request included in the Charge.	Audit and Alert Logs 60 days Operational Logs 30 days	Audit and Alert Logs 120 days Operational Logs 30 days	Audit and Alert Logs 13 month rolling period Operational Logs 30 days
Licensing and Vendor Support Agreement Management			
Ensure that all software licences and required vendor support agreements are placed and renewed when required for the third party supplier services on the Customer's behalf.	✓	✓	✓
Continuous Improvement of the Associated Services			
BT Managed Security Service and Associated Services reviews	6 monthly	Quarterly	At intervals agreed by both Parties

	Foundation	Foundation Plus	Premium
Identification of Vulnerabilities. Vulnerability Patch included in the Charge (CVSS score)	CVSS score 9 and above	CVSS score 7 and above	CVSS score 5 and above
CSP Change Management	Via Security Portal	Via Security Portal or the Security Optimisation Manager and target implementation times for changes.	Additionally to Foundation Plus; BT support for identifying errors or potential unforeseen consequences of Customers requested changes

3.2 The Graded Service Tier selected with the initial Order shall also apply for any future Orders the Customer may place for the Associated Service as the Customer cannot have more than one Graded Service Tier.

3.3 The Customer may upgrade to a higher Graded Service Tier but the Customer may not downgrade to a lower Graded Service Tier during the Minimum Period of Service or any subsequent Renewal Period subject to following conditions:

3.3.1 signature of a new Order;

3.3.2 no termination Charges will be payable from the Graded Service Tier the Customer is moving from;

3.3.3 the Minimum Period of Service will continue to apply to the upgraded Graded Service Tier; and

3.3.4 any new Charges for the upgraded Graded Service Tier will be agreed by a new Order; taking the following into account:

(a) If the Customer pays annually or quarterly in advance, the Customer will then pay BT the difference in Charges between the lower and the higher Graded Service Tiers for the period of the Minimum Period of Service or Renewal Period that the Customer has paid in advance and commence paying the new Charges for the higher Graded Service Tier from the next billing period;

(b) if the Customers pays monthly in advance, the Customer will pay BT the Charges for the higher Graded Service Tier from the billing period one month before the date of the upgrade.

3.4 If there is a conflict between the provisions of the Graded Service Tiers, the order of priority of the relevant provision, depending on the Graded Service Tier ordered by the Customer, is the following:

3.4.1 Premium;

3.4.2 Foundation Plus;

3.4.3 Foundation.

4 DELIVERY - INITIAL SETUP

BT will facilitate the setup and delivery of the Associated Services as are set out in the respective Annex of an Associated Service and as further detailed on the Order. The setup and delivery and each Party's obligations may vary depending on the respective Graded Service Tier selected with the Associated Service and the nature of the Associated Service as set out in the respective Annex of such Associated Service.

4.1 BT Obligations

Before the Operational Service Date and, where applicable, throughout the provision of the BT Managed Security Service and Associated Services, BT will:

Standard BT Obligations with Foundation

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

4.1.2 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, but BT will not be liable if, as a result of any such compliance, BT is in breach of any of its obligations under this Agreement;

4.1.3 provide standard polices that reflect good practice;

4.1.4 keep the Customer informed throughout the delivery process.

4.1.5 co-ordinate the delivery of the Associated Services;

4.1.6 revise the expected delivery date if the Customer requests a change to Associated Service before the planned delivery date to accommodate that change;

4.1.7 configure the Associated Services, if required, in accordance with the CSP(s) policies selected by the Customer.

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

4.1.9 connect the Associated Services to each Enabling Service as set out in the Annex for the relevant Associated Service;

4.1.10 if applicable for an Associated Service as set out in the respective Annex of such Associated Service,

(a) arrange for any surveys to be conducted to confirm the availability of a suitable environment for provision of the Associated Services (including confirming the presence of Enabling Services);

(b) install the BT Equipment and Customer Equipment; and

4.1.11 On the date that BT has completed the activities in this Paragraph, BT will confirm to the Customer the date that the Initial Setup is complete, that the Controlled Deployment CSP Optimisation Period has commenced and the Operational Service Date.

Additional BT Obligations with Foundation Plus

4.1.12 BT will appoint a named BT Project Manager to be the Customer's single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit the Customer's Site.

4.1.13 BT will deliver the Associated Service in accordance with the on-time Delivery Service Level as set out in Paragraph 19 of this Schedule;

4.1.14 BT will provide a customisable security policy to use as the Customer's CSPs.

Additional BT Obligations with Premium

4.1.15 BT will provide a named BT Project Manager who will be available to attend meetings at the Customer's Site depending on the Customer's location for the duration of the Initial Setup.

4.2 Customer Obligations

Before the Operational Service Date and, where applicable, throughout the provision of the BT Managed Security Service and Associated Services, the Customer:

Standard Customer Obligations with Foundation

4.2.1 will select appropriate policies to use as the Customer's CSP(s) when the Customer places the Order and ensure that the standard policies the Customer selects meet the Customer's requirements;

4.2.2 will be responsible for defining the Customer's ongoing CSP(s) beyond that set out in the policies selected by the Customer after the Operational Service Date; and

4.2.3 if for an Associated Service as set out in the respective Annex of such Associated Service a survey by BT is required and the surveys identify that additional work is required to be undertaken by the Customer in order to provide a suitable environment, the Customer will complete these works prior to installation of the applicable Associated Services. Failure to do so may result in a change to the delivery date and may require BT to provide a new quote to the Customer, detailing the additional Charges the Customer will need to pay for the additional work to be completed. In such event:

(a) where the Customer accepts 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 delivery date; or

(ii) modify the existing Order to reflect the new requirements and provide a new delivery date;

(b) where the Customer does not accept the new quote, BT will cancel the Customer's existing Order for the provision of the BT Managed Security Service or Associated Service to the affected Site(s) and BT will have no obligation to provide the BT Managed Security Service or Associated Service to that Site.

4.3 Service Options

Following Service Options are available subject such is agreed on the Order together with any additional Charges for such Service Options:

4.3.1 A named BT Project Manager. If not part of the Graded Service Tier as selected by the Customer; the Customer may request that BT appoints a named BT Project Manager to be the Customer's single point of contact during the Initial Setup. The Customer may select on the Order if such named BT Project Manager will a) undertake any activity remotely and will not visit the Customer's Site or b) be available to attend meetings at the Customer's Site. If the Customer requires a named BT Project Manager the

Customer will provide a Customer project manager and Customer technical team to work with the named BT Project Manager during the Initial Setup and the Controlled Deployment Optimisation Period; and

4.3.2 BT Professional Services. If not part of the Graded Service Tier as selected by the Customer; the Customer may request that BT provides Professional Services to assist the Customer in the creation of the Customer's CSP(s). The responsibility for the CSP(s) will however remain with the Customer.

5 DELIVERY - CONTROLLED DEPLOYMENT

5.1 **BT Obligations.** During the Controlled Deployment CSP Optimisation Period, BT will:

Standard BT Obligations with Foundation

5.1.1 prepare a deployment plan;

5.1.2 provide the Customer with User Guides for the Associated Service;

5.1.3 work with the Customer whereby BT will provide activation support to the Customer so that the Customer has access to any required Portals for configuration of the Associated Service. If BT is aware that, or the Customer advises BT that, the Customer is unable to access the BT Security Portal, BT will direct the Customer to the appropriate BT Personnel to review the Customer's request;

5.1.4 deploy the Associated Service using the agreed supply methods and, if the Customer has chosen to include the deployment services option in the Services, BT will work with the Customer to decide which method of deployment to use;

5.1.5 not provide any further support to the Customer during the Controlled Deployment CSP Optimisation Period. If the Customer has requested changes to the CSP(s) during the Controlled Deployment CSP Optimisation Period, BT will direct the Customer to the CSP change management facility on the BT Security Portal; and

5.1.6 once the Customer informs BT that the Controlled Deployment CSP Optimisation is completed, notify the Customer of the date of completion of the Controlled Deployment CSP Optimisation.

Additional BT Obligations with Foundation Plus and Premium.

5.1.7 provide any further support to the Customer in carrying out the Controlled Deployment CSP Optimisation.

5.2 **Customer Obligations.** During the Controlled Deployment CSP Optimisation Period, the Customer will:

5.2.1 be responsible for carrying out the Controlled Deployment CSP Optimisation within the Controlled Deployment CSP Optimisation Period in compliance with the User Guides;

5.2.2 notify BT when the Customer has completed the Controlled Deployment CSP Optimisation. If the Customer does not provide BT with such notice by the end of the Controlled Deployment CSP Optimisation Period, the Controlled Deployment CSP Optimisation will be deemed to have been completed by the Customer; and

5.2.3 submit any changes the Customer requires to the CSP as a result of the Controlled Deployment CSP Optimisation through the CSP Change Management Process.

6 IN LIFE - MONITORING AND MANAGEMENT – SECURITY THREAT INTELLIGENCE

6.1 **BT Obligations.** On and from the Operational Service Date, BT will provide with each Graded Service Tier the following general intelligence bulletins and reports in English to an agreed list of Customer Contacts:

6.1.1 daily threat advisories: these provide a view of the latest headline security events, actors, targets, operations and campaigns, vulnerabilities and suspicious IP Addresses;

6.1.2 global threat summaries: these provide a wide angle and high-level view of the significant events and attacks that have occurred globally and across all industries;

6.1.3 monthly executive level briefing: these provide a CISO level view of the threat landscape focussing on events impacting global organisations from a strategic perspective; and

6.1.4 global critical bulletins: these provide a technical assessment of significant global security events such as WannaCry so that a more detailed understanding can be obtained.

6.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will be responsible for resolving the issues that BT provides the Customer advance warning of as part of above Security Threat Intelligence.

7 IN LIFE - MONITORING AND MANAGEMENT – PROACTIVE MONITORING

The following is only applicable for Associated Services where the respective Service Annex explicitly includes proactive monitoring with the Associated Service.

7.1 **BT Obligations.** On and from the Operational Service Date, BT will:

Standard BT Obligations with Foundation

7.1.1 monitor the performance of the Associated Services at intervals set by BT and, where possible, provide advance warning to the Customer through the BT Security Portal of impending issues that may affect an Associated Service and that BT identifies as a result of the monitoring. BT may not identify all impending issues;

7.1.2 check that the Associated Services are operating correctly by;

(a) polling the Security Appliance to check it is powered on and has network connectivity. If the Security Appliance is not powered on or does not have network connectivity, the SOC will investigate and either take appropriate action or recommend action that the Customer requires to take;

(b) Security Appliance status test: BT will test at regular intervals at BT's discretion as follows:

(i) Resource status: conduct one (1) test per resource per Security Appliance such as CPU and RAM;

(ii) physical status: conduct one test per physical attribute per Security Appliance such as temperature, where applicable to the Security Appliance;

(iii) compare test results against standard vendor thresholds and notify any variances to the SOC. The SOC will investigate and either take appropriate action or recommend action that the Customer is required to take;

(c) access monitoring: generate alerts in near real time for unauthorised access attempts; and

(d) application update status: on UTM/IDS/URLF and other applications selected as part of the Associated Service;

Additional BT Obligations with Foundation Plus

7.1.3 agree with the Customer a process to contact the Customer when it identifies an issue that impacts the Associated Services.

7.1.4 in addition to any other checks carried out by BT under Foundation, check that the Associated Services are operating correctly by monitoring the applications under the relevant Associated Services against parameters set by BT.

Additional BT Obligations with Premium

7.1.5 in addition to any other checks carried out by BT under Foundation and Foundation Plus; check that the Associated Services are operating correctly by:

(a) password management including checking age and complexity of passwords, along with checking password hashes against known leaked password hash databases; and

(b) certificate expiry monitoring, while the Customer remains responsible for updating certificates.

7.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will:

7.2.1 be responsible for resolving the issues that BT provides the Customer advance warning of; and

7.2.2 ensure that the Customer or third parties, as required, configure routing/permissions on platforms or Associated Services to allow BT to carry out the monitoring.

8 IN LIFE - MONITORING AND MANAGEMENT – MANAGE SERVICE INCIDENTS.

8.1 **BT Obligations.** On and from the Operational Service Date, BT will act as a single point of contact for resolution of Incidents related to the Associated Service; depending on the respective Graded Service Tier selected by the Customer whereby BT will:

Standard BT Obligations with Foundation

8.1.1 operate a Service Desk that will action any Incident notifications and which is available 24 hours a day; 7 day per week and staffed by security trained professionals. All communications with the Service Desk will be in English;

8.1.2 accept only Incidents raised by the Customer via the BT Security Portal if the Customer only ordered Foundation;

8.1.3 give the Customer a Ticket if BT identifies an Incident;

8.1.4 assess the Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	One or more core Sites or Services are completely unavailable, or one or more core functions of the Associated Services are completely unable to be performed. For User-based services (e.g. MS Teams), this would typically be all Users.
P2	Material impact to Associated Service e.g., a partially interrupted or impaired Service which cannot be mitigated, or core business functions can be performed but in a reduced capacity. This priority level would also apply for the loss of a non-core site or Service.
P3	Medium impact to Associated Service, e.g., a Site or Service experiencing intermittent or localised interruption or impairment. This might be an issue where a large percentage of the Associated Service is functioning normally, such as the Site is suffering slow response, but Users are able to work, a small number of Users at a Site have total loss of service but the majority are functioning normally, or perhaps one element of Service is unavailable, such as access to voicemail. A P3 incident would also be raised for a resilient Site where either the primary or resilient path is unavailable.
P4	Typically very minor or no impact on Associated Services, such as a single User or very small number of Users having minor issues but core functions of the Associated Services can be carried out as normal.

8.1.5 respond to Incidents and aims to the provide the Customer with any an update on the progress of an Incident, in line with the following table and this starting from when the Service Desk provides the Customer with a Ticket:

	Incident Stage			
Priority	**Initial Response**	**Next Response**	**Further Responses**	**Target Restoration**
P1	the Customer will be informed that BT is dealing with the Incident within 15 minutes of receiving it (either via an alert or by the Customer advising BT)	First update within 30 minutes from the Incident ticket being opened	Every 60 minutes	4 hours
P2	the Customer will be informed that BT is dealing with the Incident within 30 minutes of receiving it (either via an alert or by the Customer advising BT)	First update within 60 minutes from the Incident ticket being opened	Every 2 hours	8 hours
P3	N/A	First update within 4 hours from the Incident ticket being opened	Every 4 hours	24 hours
P4	N/A	First update within 24 hours from the Incident ticket being opened	Every 24 hours	48 hours

Note: the response times and restoration times are targets only and BT will have no liability for failure to meet them.

8.1.6 review the status of the Incident and amend the priority level assigned initially if necessary;

8.1.7 keep the Customer informed throughout the course of the Incident resolution at regular intervals by posting updates on the BT Security Portal or via e-mails to the Customer Contact. However, BT will not provide a progress update while BT is waiting on Customer's input or feedback and the ticket will be put into pending status. The total time when the ticket is in pending status will be excluded when measuring both response and restoration timings and when measuring availability of the Service.

8.1.8 be responsible for closing Tickets for an Incident in accordance with following process:

(a) if BT believes the Incident is cleared; BT will close the Ticket when:

(i) the Customer confirms that the Incident is cleared, or

(ii) BT has attempted unsuccessfully to contact the Customer Contact and the Customer Contact has not responded within 24 hours following BT's attempt to contact the Customer Contact. BT will attempt to contact the Customer Contact three times in total, at regular intervals, before automatically closing the Incident Ticket.

(b) if the Customer confirms that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident;

8.1.9 where applicable, maintain back-up configurations to allow all the Associated Service to be restored fully following the swap out of a Security Appliance.

Additional BT Obligations with Foundation Plus

8.1.10 agree with a Customer a process to contact the Customer when it identifies an issue that impacts the Associated Service.

8.1.11 accept Incidents raised by the Customer via a) the BT Security Portal or b) directly by telephone to the Service Desk, but not the ones raised to the regional Security Operations Centre;

8.1.12 be responsible for checking that the Associated Service is operating correctly by monitoring the applications under the Associated Service against parameters set by BT.

Additional BT Obligations with Premium

8.1.13 once BT receives an alert; remediate where accessible and possible, as agreed with the Customer and to the extent defined in the CSP.

8.1.14 accept Incidents raised by the Customer via a) the BT Security Portal or directly by telephone to b) the Service Desk or c) the regional Security Operations Centre;

8.1.15 once the Incident is resolved, assist the Customer with the modification of its CSP to avoid any further recurrences of the same Incident.

8.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will:

8.2.1 where the Customer becomes aware of an Incident; ensure that the Customer Contact will report any Incidents in accordance with the Incident reporting methods available with the selected Graded Service Tier;

8.2.2 allow BT to run discovery tools on the Customer's network to enhance and fine tune the Customer's CSP(s) or to assist in the resolution of Incidents.

9 IN LIFE - MONITORING AND MANAGEMENT – SIGNATURE UPDATES

The following is only applicable for Associated Services where the respective Service Annex explicitly includes Signature Updates with the Associated Service. Such will apply for Foundation, Foundation Plus and Premium.

9.1 **BT Obligations.** On and from the Operational Service Date, BT will:

9.1.1 identify and implement Signature Updates on Associated Services at a time convenient to BT;

9.1.2 where possible, identify and apply an automated method for applying Signature Updates unless this may impact the Associated Services;

9.1.3 if BT is aware that the Customer's Associated Services will have downtime or that the Signature Update will cause an impact on the Associated Services or if the Signature Update needs to be done manually, BT will contact the Customer to agree on an appropriate time within Business Hours for the Signature Update to be applied;

9.2 **Customer Obligations.** On and from the Operational Service Date, Customer will:

9.2.1 provide consent to BT applying the Signature Updates automatically;

9.2.2 request or authorise BT to reverse the Signature Update if it causes an Incident in the Associated Service;

9.3 **Service Option.** Signature Updates outside Business Hours are possible subject to agreement by an Order and any applicable Charges for such Signature Updates outside Business Hours.

10 IN LIFE - MONITORING AND MANAGEMENT – LOG CAPTURE

The following is only applicable for Associated Services where the respective Service Annex of the Associated Service explicitly includes Log Capture.

10.1 **BT Obligations.** On and from the Operational Service Date, BT will:

Standard BT Obligations with Foundation

10.1.1 implement a logging capability on Associated Services where the standard design of the Associated Services allows the capture of logs through standard process.;

10.1.2 capture and store a minimum log set to enable BT to offer effective management of Associated Services;

10.1.3 make the captured logs available to the Customer if the Customer requests access to the logs in accordance with this Paragraph 9;

10.1.4 store the Audit and Alert Logs within an appropriate secure BT environment outside of the Customer's environment on a rolling 13 month basis where appropriate;

10.1.5 store the Operational Logs within an appropriate secure BT environment outside of the Customer's environment on a rolling one month basis where appropriate;

10.1.6 make available the previous 60 days' Audit and Alert Logs to the Customer on the Customer's request;

10.1.7 make available the previous 30 days' Operational Logs to the Customer on the Customer's request;

10.1.8 use reasonable endeavours to transmit and store the logs securely.

10.1.9 store the logs in their raw state or compress them if appropriate.

Additional BT Obligations with Foundation Plus

10.1.10 make available the previous 120 days' Audit and Alert Logs to the Customer on the Customer's request.

10.1.11 make logs available to:

(a) the Customer's, or third party technologies, where appropriate as agreed with the Customer; or
(b) to other services BT is providing to the Customer that do not form part of the Agreement where appropriate as agreed with the Customer.

Additional BT Obligations with Premium

10.1.12 make available Audit and Alert Logs to the Customer on the Customer's request for a rolling 13 month period.

10.2 **Customer Obligations.** On and from the Operational Service Date, Customer will confirm the Customer's specific logging requirements at the time of placing the Order.

10.3 **Service Option.** Subject to agreement of an Order including any additional Charges; the Customer may require Log Capture according to Customer's specific requirements which are not standard supported by BT; including but not limited to:

9.3.1 access to the logs outside of the days as set out under the order Graded Service Tier selected;

9.3.2 logs to be sent to and to be stored in a repository on the Customer's Site or third party premises based on a design as agreed between Parties; subject to the condition that:

(a) the Customer will be responsible for the logs while they are sent to or stored in such a repository;
(b) the other obligations of BT as set out in Paragraph 9.1 will not apply to logs sent to or stored in such a repository;
(c) the Customer will take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with BT; and
(d) the Customer will ensure that the Customer or the nominated third party uses reasonable endeavours to secure the repository appropriately.

11 IN LIFE – MONITORING AND MANAGEMENT – LICENSING AND VENDOR SUPPORT AGREEMENT MANAGEMENT

The following is only applicable for Associated Services where the respective Service Annex of the Associated Service explicitly includes Licensing and Vendor Support Agreement Management for third party licenses provided with the Associated Service. Such will apply for Foundation, Foundation Plus and Premium.

11.1 **BT Obligations.** On and from the Operational Service Date, BT will:

11.1.1 ensure that all software licences and required vendor support agreements are placed and renewed when required for the third party supplier services on the Customer's behalf.

11.1.2 provide, implement and deploy appropriate licences and required vendor support agreements for the third party supplier services on the Customer's behalf.

11.1.3 be responsible for ensuring software licences and any required vendor support agreements are renewed for the term of the Agreement.

11.1.4 in the event the Parties agree on a Renewal Period, renew the software licence or required support agreement for a period for a period of twelve (12) months or as otherwise agreed by both Parties in an Order.

11.1.5 validate that the Customer has ordered the correct number of licences either direct from the third party supplier or through BT to serve the Customer's requirements for the relevant the third party supplier services in accordance with terms of the software licences and vendor support agreements and information provided by the Customer and:

(a) if BT determines that the Customer has not ordered sufficient licences either direct from the vendor or through BT for a the third party supplier service, BT will notify the Customer and the Customer 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 relevant Associated Service and subsequently terminate the Associated for material breach as set out in the General Terms and Conditions of the Agreement; and
(c) BT will not be liable for unknown breaches of the software licences and vendor support agreements, where BT is acting on information provided by the Customer.

11.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will confirm to BT any change in the number of Users requiring licences as part of the Supplier Services.

12 IN LIFE - CONTINUOUS IMPROVEMENT - REVIEWS.

The following is only applicable for Associated Services where the respective Service Annex of the Associated Service explicitly includes Continuous Improvements with Review.

12.1 **BT Obligations.** On and from the Operational Service Date, BT will carry out below reviews to the Customer as additional Continuous Improvement service depending on the Graded Service Tier as selected by the Customer on the Order.

Standard BT Obligations with Foundation

12.1.1 The Security Optimisation Manager will carry out a review six (6) monthly as follows:

(a) a service review focussing on the performance of the BT Graded Service Tier and the Associated Service; and

(b) an end of life review on an ongoing basis. The Security Optimisation Manager will provide the Customer with a report summarising the applications and software that are managed by BT on the Customer's behalf as part of the Associated Service that will go end of life within the following six months. The report will include applications and software advised to the Customer previously that are past end of life and that require immediate action by the Customer.

Additional BT Obligations with Foundation Plus

12.1.2 The Security Optimisation Manager will carry out a review quarterly as follows:

(a) a service review focussing on the performance of the BT Graded Service Tier and the Associated Service against Service Targets and capacity management of the Associated Service; and

(b) a review of the Customer's CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of the Customer's CSP(s).

12.1.3 Upon Customer's request the Security Optimisation Manager will attend a conference with the Customer to discuss the report.

Additional BT Obligations with Premium

12.1.4 The Security Optimisation Manager will carry out the reviews as set out in Paragraph 12.1.1 and 12.1.2 at intervals agreed by both Parties but not less than monthly;

12.1.5 The Security Optimisation Manager will provide the Customer with a report on the review via the BT Portal or direct to the Customer by e-mail, if agreed by both Parties; and

12.1.6 Upon Customer's request the Security Optimisation Manager will attend a meeting with the Customer to discuss the report.

12.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will:

12.2.1 take appropriate action to address issues as recommended by the Security Optimisation Manager including:

(a) implementing security improvements as agreed with the Security Optimisation Manager or as advised by the Security Optimisation Manager as the Customer's responsibility;

(b) initiating the appropriate change requests in accordance with the CSP Change Management Process to address issues in respect of fine tuning or amending the Customer's CSP(s) as recommended by the Security Optimisation Manager; and

(c) any action in respect of the end of life review or as set out in the end of life review report.

12.2.2 if the Customer requested a conference call or a meeting with the Security Optimisation Manager to discuss the report; ensure that any report the Security Optimisation Manager provides the Customer with will be reviewed by the Customer's suitably qualified personnel who are participating in the conference call or the meeting prior to the conference call or meeting taking place.

13 IN LIFE - CONTINUOUS IMPROVEMENT - VULNERABILITY MANAGEMENT AND PATCHING OF SECURITY APPLIANCES

The following is only applicable for Associated Services where the respective Service Annex of the Associated Service explicitly includes Continuous Improvements with Vulnerability Management and Patching of Security Appliances. Vulnerability Management and Patching of Security Appliances will only be available while the Security Appliance is supported by the vendor. The Patch updates will be ranked in accordance with following CVSS Score:

CVSS Score	Qualification
5.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10	Critical

13.1 **BT Obligations.** On and from the Operational Service Date, BT will:

Standard BT Obligations with Foundation

13.1.1 implement a Patch for a Vulnerability with a Critical CVSS score, subject to the Customer's agreement and also agreeing an implementation time slot with the Customer;

13.1.2 only accept through the BT Security Portal communications in respect of Vulnerability Management and Patching of Security Appliances;

13.1.3 provide a secure mechanism on the BT Security Portal for the Customer to confirm the Customer's agreement to BT implementing a Patch that BT has recommended;

13.1.4 specify an implementation window for BT to implement the Patches which will be typically a weekly six hour window outside of Business Hours for the Site where the Security Appliance is situated;

13.1.5 apply the Patch in the specified implementation window and confirm to the Customer via the Security Portal when the Patch has been implemented;

13.1.6 roll the Patch back upon the Customer's request in the event that the Customer detects undesirable side-effect;

13.1.7 not assess the configuration or contextual exposure of any Security Appliances to the Vulnerability;

Additional BT Obligations with Foundation Plus

13.1.8 implement a Patch for a Vulnerability with a Critical CVSS score and a High CVSS score and the latest stable variant of the vendor's general availability code, subject to the Customer's agreement and also agreeing an implementation time slot with the Customer.

Additional BT Obligations with Premium

13.1.9 implement a Patch for a Vulnerability with a Critical CVSS score, a High CVSS score and a Medium CVSS score and the latest stable variant of the vendor's general availability code, subject to the Customer's agreement and also agreeing an implementation time slot with the Customer;

13.2 **Customer Obligations.** On and from the Operational Service Date, the Customer will:

13.2.1 will assess the suitability for deployment of the Patches that BT advises are available to address notified Vulnerabilities within the Customer's specific environment and for any post-implementation testing;

13.2.2 provide consent to BT allowing BT to accept and implement a Patch within 14 days of notification by BT of a recommended Patch. If the Customer refuses to provide such consent or requests that an installed Patch is reversed out due to the Customer's specific undesirable side-effects, BT will be under no further obligation to provide further Vulnerability Management and Patching in respect of that Patch and will not have any liability for potential exposure should a threat subsequently exploit that related Vulnerability.

13.3 **Service Options.** Subject to agreement of an Order including any additional Charges;

13.4 the Customer who ordered Foundation may require from BT also to implement Patches for a Vulnerability with a High CVSS score and a Medium CVSS score;

13.5 the Customer who ordered Foundation Plus may require from BT also to implement Patches for a Vulnerability with a Medium CVSS score.

14 IN LIFE - CSP CHANGE MANAGEMENT PROCESS

14.1 **BT Obligations.** On and from the Operational Service Date, BT will implement changes to the CSP(s) in response to Customer's request subject to the following process ("CSP Change Management Process"). The CSP Change Management Process may vary depending on the nature of the change, the respective Associated Service and the Graded Service Tier selected by the Customer as set out on the Order. BT makes a distinction between following types of changes:

14.1.1 Simple Changes – Standard: A Standard Change is a Simple Change relating to upgrades and modifications needed as a result of planned developments and security improvements. Standard Changes will be implemented by BT according to the timelines as agreed in the CSP subject to Customer's prior approval.

14.1.2 Simple Changes – Urgent: An Urgent Change is a Simple Change relating to 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 will be implemented by BT as soon as reasonable practicable subject to Customer's prior approval.

14.1.3 Simple Changes – Emergency: A Emergency Change is a highly critical, Simple Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to business operations, or to prevent or resolve a P1 Incident. An Emergency Change will be implemented by BT as

quickly as reasonably practicable but without Customer's prior approval; subject that BT afterwards demonstrate why such Emergency Change was required.

14.1.4 Complex Changes are changes which according to the respective Associated Service not defined as a Simple Change and therefore Complex Changes will be agreed - including any additional Charges for implementing such Complex Changes - via a new Order;

Standard BT Obligations with Foundation

14.1.5 BT will only accept requested changes raised by the authorised Customer Contact via the BT Security Portal.

14.1.6 BT will check each request for its complexity and assess whether the change (i) should be completed via the CSP Change Management Process, (ii) requires a new Order or (iii) requires a contract change to be agreed by a written amendment to the Agreement.

14.1.7 If BT is aware that, or the Customer advises that, the Customer is unable to access the BT Security Portal, BT will direct the Customer to the appropriate BT personnel to review the Customer request.

14.1.8 Only CSP changes to rule-sets that define the operation of the Service will be completed via the CSP Change Management Process.

14.1.9 For the avoidance of doubt; any change whereby the Customer requests changes to the Service not being qualified as Simple Change (e.g. including additional licences) requires a new Order.

14.1.10 A number of Simple Change are included in the Charges subject to the limitations as set out with the respective Associated Service (called "**Reasonable Use Policy**"). The number of Simple Changes included in the Charges may vary depending on the respective Associated Service and the Graded Service Tier selected by the Customer as set out on the Order. Where Standard and/or Urgent Changes are being raised more frequently by the Customer; the Parties may either agree:

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

(b) to review the Customer requirements and agree with the Customer an appropriate alternative implementation process and any associated charges via a new Order; or

(c) to charge such additional change request at the rate as set out in the Order.

14.1.11 BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change and the status will be available also on the BT Portal for a period of six months.

Additional BT Obligations with Foundation Plus

14.1.12 BT will accept requested changes raised by the authorised Customer Contact via the BT Security Portal and/or direct via the Security Optimisation Manager.

14.1.13 BT will aim to implement changes to the Customer's CSP(s) in accordance with the table set out below:

Request	Target Implementation Time
Simple Change - Standard Change	8 Hours calculated from the moment BT accepted the Customer's change request.
Simple Change - Urgent Change	4 Hours calculated from the moment BT accepted the Customer's change request.
Simple Change - Emergency Change	4 Hours calculated from the moment identified the need for an Emergency Change.
Complex Change	As agreed on the Order

Additional BT Obligations with Premium.

14.1.14 BT will aim to identify any errors or potential unforeseen consequences of Customers requested Simple Changes and Complex Changes.

14.2 **Customer Obligations.** On and from the Operational Service Date, the Customer:

14.2.1 will ensure that only the authorised Customer Contact will submit requests to change the CSP(s) and will provide sufficient detail and clear instructions as to any changes required. The Customer will not, and ensure that Users with access to the BT Portal do not, submit any unauthorised changes;

14.2.2 except for Emergency Changes,

(a) the Customer is deemed to have approved all changes to the CSP(s) that are submitted to BT; and

(b) will be responsible for the impact of BT implementing the changes. This means if BT implements this change in accordance with the Customer request, BT will not be liable for any

consequences arising from the impact of the implementation of the changes; including any misspecification of the Customer security requirements in the CSP(s) or any unforeseen consequences of a correctly specified and correctly implemented CSP(s).

14.3 **Service Option**. The Customer may order Professional Services from BT to assist the Customer in writing the change request.

15 IN LIFE - REPORTING

15.1 **BT Obligations.** On and from the Operational Service Date, for each of the selected Graded Service Tier BT will:

15.1.1 provide the Customer with an inventory of and reporting for Associated Service via the BT Security Portal, including:

(a) a dashboard tailored to the Associated Service; and
(b) appropriate inventory information.

15.1.2 provide reports with details and at a frequency as appropriate on:

(a) usage and capacity management of the Associated Service, where applicable; and
(b) end of life and end of service of security appliances, firmware and operating systems.

16 OPTIONAL PROFESSIONAL SERVICES

16.1 With BT Managed Security Services (as set out in this Service Schedule) and with a specific Associated Service (as set out in the respective Annex of such Associated Service); the Customer may order additional Professional Services from BT to assist the Customer with several task set out to be a Customer obligation.

16.2 Additional Professional Service is chargeable and shall be ordered separately whereby the details of such additional ad-hoc Professional Service and the applicable Charges (which may be a fixed or a rate chargeable per day) will be set out in the applicable Order.

16.3 Professional Services are delivered remotely unless otherwise set out in the Order.

16.4 Professional Services are provided on a reasonable endeavours basis and shall not be considered as a commitment of result.

17 ADDITIONAL OBLIGATIONS FOR EACH PARTY

17.1 **IP Addresses and Domain Names**

17.1.1 Except for IP Addresses expressly registered in the Customer's 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 are non-transferable.

17.1.2 All of the Customer's rights to use such IP Addresses or Domain Names will cease on termination or expiration of the Service.

17.1.3 BT cannot ensure that any requested Domain Name is available from or approved for use by the applicable Regional Internet Registry and BT has no liability for any failure in the Domain Name registration, transfer or renewal process.

17.1.4 The Customer will not use IP Addresses that the Customer does not own or that are incorrectly specified and the Customer will be responsible for the use of IP Addresses within the Customer's network. BT may apply additional Charges for dealing with changes or Incidents that occur as a result of incorrect / illegal IP Addressing schemes.

17.1.5 The Customer warrants that the Customer is the owner of, or are authorised by the owner of, the trade mark or name that the Customer wishes 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.

17.1.6 The Customer will pay all fees associated with registration and maintenance of the Customer's Domain Name, and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

17.2 **Employer Disclosure.** In jurisdictions where an employer is legally required to make a disclosure to its Users and other employees (also called "employer disclosure"), the Customer will:

17.2.1 inform the Users (individually or via local workers councils depending on applicable law) that as part of the Service being delivered by BT, BT may monitor and report to the Customer the use of any targeted applications by them;

17.2.2 ensure that the Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required) in accordance with applicable law; and

17.2.3 be liable to BT for any claims, losses, costs or liabilities incurred or suffered by BT due to Customer's failure to comply with this Paragraph.

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

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

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

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

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

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

17.3.5 Where the EULA(s) is presented in a 'click to accept' function and the Customer requires BT to configure or install Software on the Customer`s behalf, BT will do so as the Customer`s agent and bind the Customer to the EULA(s). For this purpose, the Customer hereby already grants to BT a mandate to enter into the EULA(s) in the Customer's name and on its behalf. BT and the Customer may for this also execute a power of attorney as part of the Order.

17.4 **Maintenance.** BT may carry out Planned Maintenance from time to time and will use reasonable endeavours to inform the Customer at least five (5) Business Days before any Planned Maintenance on the Service. For the avoidance of doubt any emergency maintenance shall not be considered as Planned Maintenance. Emergency maintenance and related updates and other procedures will be scheduled by BT, on a case-by-case basis. Advance notice of emergency maintenance will be given to the Customer where reasonably practicable. If it is not possible to give advance notice BT will inform the Customer after why emergency maintenance was required without advance notification.

17.5 **Customer IDs and passwords.**

17.5.1 The Customer will provide to BT any account names and passwords necessary to install and commission the Service.

17.5.2 BT will maintain any relevant BT Security Portal and server to provide the Customer with online access to a range of functions including performance reports and placing CSP change requests.

17.5.3 The Customer may request from BT up to five (5) login/password combinations for access to the BT Security Portal, for use by the Customer or its agents. The Customer will maintain a written list of current Customer's employees receiving access and provide a copy of such list to BT within five (5) Business Days following BT's written request at any time.

17.5.4 At the Customer's sole discretion, the Customer may assign one (1) login combination to BT Personnel. The Customer is responsible for its agents' use of these IDs.

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

(a) allow anyone else to use their administrator specific subscription, token/ID or share passwords unless it has been reassigned in its entirety to another individual administrator, in which case the Customer will ensure the prior administrator will no longer have any right to access or use the Service;
(b) leave their User account logged in while the computer is unattended and unlocked;
(c) submit any unauthorised changes; or
(d) attempt to access data that they are not authorised to access; or

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

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

18 SERVICE MANAGEMENT BOUNDARY

18.1 BT will provide and manage the BT Managed Security Service in accordance with this Schedule and the Associated Services up to the Service Management Boundary as set out in the applicable Annex for the Associated Service.

18.2 BT will have no responsibility for the BT Managed Security Service outside the Service Management Boundary.

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

18.4 Where BT is required to link to or utilise a non-BT provided network to enable BT to provide the BT Managed Security Service to the Customer, and there is a subsequent failure to the third party network which causes disruption to the BT Managed Security Service, BT will have no liability to the Customer relating to provision and performance of the BT Managed Security Service and BT's inability to provide the BT Managed Security Service, or its effect on other Associated Services. If BT is required to carry out additional work to resolve any issues arising, the Parties will agree the additional work and additional Charges for such work in writing. The Service Levels and Service Targets will not apply.

19 CHARGES, MINIMUM PERIOD OF SERVICE, RENEWAL AND TERMINATION CONDITIONS

19.1 The Charges for a selected Graded Service Tier and any options shall be set out on the Order with the Associated Service.

19.2 In addition to the Charges as set out on the Order; BT is entitled to charge the Customer any costs incurred by BT due to the Customer:

19.2.1 if Site visits were agreed, aborting any Site visit as planned by BT;

19.2.2 cancelling or amending orders whereby BT has ordered equipment from a supplier to fulfil BT's obligations and BT is unable to return the equipment to the supplier;

19.2.3 asking BT to perform work outside Business Hours, except if this part of the ordered Graded Service Tier;

19.2.4 reporting Incidents to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Agreement, including where the Incident has arisen as a result of the Customer changing the Customer's CSP(s;

19.2.5 requiring from BT to link or utilise a non-BT provided network to enable BT to provide the Service to the Customer, and there is a subsequent failure to the third party network which causes disruption to the Service resulting that BT is required to carry out additional work to resolve any issues arising;

19.2.6 requiring BT for expediting the provision of the service after BT has informed the Customer of the target delivery date;

19.2.7 being in breach of its obligations resulting that BT needed to restore the service after BT has suspended the service due to Customer's breach in accordance with the Agreement. This may include the costs BT incurred from a supplier or vendor:

(d) for reinstating any lapsed software licences or required vendor support agreements where the licences or support agreements have lapsed as a result of any action the Customer has taken or not taken or not complying with BT's instruction; or

(e) if the Customer cancels or terminates the software licence or vendor support agreement during the Minimum Period of Service or any renewal period.

19.3 The applicable Minimum Period of Service, renewal and termination conditions for BT Managed Security Services shall be the same as for the Associated Service as set out on the respective Annex for such Associated Service.

20 SERVICE LEVELS

20.1 **Introduction**. For each Associated Service where the Customer has ordered Foundation Plus or Premium as Graded Service Tier; BT will provide an On-Time Delivery Service Level. Other Service Levels may apply for a specific Associated Service. In such event this will be set out in the respective applicable Annex of such Associated Service.

20.2 **On-Time Delivery Service Level**.

20.2.1 On-Time Delivery is the Service Level whereby BT will ensure that the Associated Service (including any related BT Managed Security Services) are delivered and installed within the Customer Committed Date.

20.2.2 The Customer may request a delivery date on the Order for each Site, the "Customer Requested Date" ("CRD"). BT will respond with a Customer Commit Date ("CCD"), which is the date on which BT agrees to deliver the Service.

20.2.3 If Delivery of the Service occurs after the CCD the Customer may claim until the effective the Operational Service Date a Service Credit equal to €110.00 per Business Day for each Associated Service that fails to meet the On Time Delivery Service Level up to a maximum amount equal to the installation Charges for that Associated Service.

20.3 **Service Level conditions and general exclusions**.

20.3.1 The Service Levels do not apply:

(a) to access to the reports made available via the BT Security Portal or the ability to request CSP changes via the BT Security Portal.
(b) if the Customer does not provide access, delays providing access or denies permission for BT or its agents and suppliers to repair the Associated Service;
(c) during any trial period of an Associated Service or any part thereof which has a Minimum Period of Service less than 12 months;
(d) to failures due to a force majeure event as set out in the General Terms and Conditions;
(e) to any Qualifying Incident not reported in accordance with BT's incident reporting procedures;
(f) the Incident has arisen as a result of the Customer changing the Customer's CSP(s);
(g) due to any additional events or circumstances set out in the any applicable Associated Services Annex(es;
(h) in the event of restrictions or preventions by applicable law, a court order, an application for interlocutory relief or injunction; or
(i) if the Customer is in material breach of its obligations under the Agreement

20.3.2 The Customer agrees that BT may expedite Delivery either for operational reasons or in response to a Customer request. This will not affect the original CCD and no Service Level will apply to any expedited date. In such circumstances, the Customer agrees that the expedited Delivery date shall be the Operational Service Date.

20.3.3 If the Customer requests a change to the Service or any part of the Associated Service, BT reserves the right to change the CCD and the Service Level for the original CCD will no longer apply.

20.3.4 No Service Levels apply to CSP change requests and Vulnerability Management and Patching of Security Appliances.

20.3.5 Service Credits are limited to the 100% the monthly Recurring Charges for affected Services and are the Customer's sole right and remedy if BT does not meet the Service Levels.

20.3.6 Only BT's measurements shall be used to calculate Service Credits.

20.3.7 The sole failure by BT to meet the Service Levels is not considered being a material breach of the Agreement.

20.4 **Claiming and Payment of Service Credits**

20.4.1 To qualify for Service Credit(s), and before any Service Credit(s) can be applied, the Customer must make a claim, providing details of the reason for the claim, within 25 days of the end of the Month in which poor performance occurred.

20.4.2 Service Credits will be made by:

(a) deducting the Service Credit from the Customer's invoice within two billing cycles of a claim being received;
(b) if related to Service Credits are only related to On-Time Delivery and no Services are delivered yet; deducting the Service Credit from the first invoices following the Operational Service Date; or
(c) following termination of the Agreement where no further invoices are due to be issued by BT, direct payment by BT within two months of a claim being received and validated.

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