BT Cloud SIEM
Annex to the Managed Service Schedule

Contents

BT Cloud SIEM Service Annex to the Managed Service Schedule

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the BT Cloud SIEM Service. The terms of this Annex apply in addition to the terms set out in:

(a) the Managed Service Schedule; and

(b) the General Terms.

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Annex have the meanings given to them in the General Terms and the Schedule.

Part A – The BT Cloud SIEM Service

1 Service Summary

1.1 BT will provide you with a security information and event management service, supporting threat detection, compliance reporting, and incident response and investigation by collection and analysis of historical data across a variety of sources ("**BT Cloud SIEM Service**").

2 Managed Service Packages

2.1 You will choose one of the Managed Service Packages, some of the features of which are set out in the table below, to use with your BT Cloud SIEM Service as set out in any applicable Order. The Managed Service Package you have chosen for the BT Cloud SIEM Service must align with the Managed Service Package you have chosen for your overall Managed Service, as set out in the Schedule:

		MS1 Package	MS2 Package	MS3 Package
Initial Setup of the BT Cloud SIEM Service in accordance with Paragraph 2.4				
SIEM Appliance Delivery Model				
Cloud SIEM		✓	✓	✓
Custom Rules				
Number of additional Custom Rules		3	15	30
Controlled Deployment of the BT Cloud SIEM Service in accordance with Paragraph 2.5				
Controlled Deployment Custom Rules Optimisation Period		Up to 90 Business Days	Up to 90 Business Days	Up to 90 Business Days
Acceptance Tests		During Controlled Deployment Custom Rules Optimisation Period	During Controlled Deployment Custom Rules Optimisation Period	During Controlled Deployment Custom Rules Optimisation Period
BT & Customer joint Custom Rules test and tune		x	✓	✓
SOM	**Implementation Stage**	Review and sign off of Custom Rules	Review and sign off of Custom Rules	Review and sign off of Custom Rules
	In-Life	N/A	Shared	Named
Technical Incidents and Fault Management				
Service Desk 24x7x365		✓	✓	✓
Proactive Monitoring				
Monitor for impending issues that may affect the BT Cloud SIEM Service		✓	✓	✓
Log Capture in respect of the BT Cloud SIEM Delivery Model				

	MS1 Package	MS2 Package	MS3 Package
Log availability on request included in the Charge	90 days	90 days	90 days
Continuous Improvement of the BT Cloud SIEM Service in accordance with Paragraph 2.7			
BT Cloud SIEM Service reviews	6-monthly	Monthly	At intervals agreed by both of us but not less than monthly
Change Management	via email	via email or direct to SOM	via email or direct to SOM

2.2 The provisions in respect of MS1 will apply to MS2 and MS3 and the provisions of MS2 will apply to MS3. If there is a conflict between the provisions of the Managed Service Packages, the order of priority of the relevant provisions is:

(a) MS3;
(b) MS2; and
(c) MS1.

2.3 **Delivery Model**

The Service will be delivered via the Cloud SIEM Delivery Model set out below, as set out in any applicable Order:

2.3.1 **BT Cloud SIEM Delivery Model**

(a) BT will provide you with a cloud hosted BT Cloud SIEM Service that will include:

(i) a cloud-based Event Correlation engine that will correlate incoming Events and categorise each Event according to its severity for inspection by the BT SOC;
(ii) one or more BT Virtual Sentries or Hardware Sentries, as set out in any applicable Order, for real time collection of Event Log Data from the monitored External Data Sources;
(iii) Cloud Log Management providing on-line Log retention for up to 90 calendar days; and
(iv) Strong Access Control through role-based access features and two factor User authentication.

2.4 **Initial Setup**

BT will facilitate the setup and delivery of the BT Cloud SIEM Service in accordance with the Delivery Model and Managed Service Package selected by you, as set out in the Order.

2.4.1 **MS1**

(a) BT will provide you with access to the Security Portal for up to a maximum of five Users.
(b) BT will appoint a SOM to be your single point of contact during the Initial Setup and Controlled Deployment. The SOM will undertake any activity remotely and will not visit your Site.
(c) You may request that BT, at an additional Charge:
(i) appoints a named BT Project Manager to be your single point of contact during the Initial Setup. The named BT Project Manager will undertake any activity remotely and will not visit your Site; or
(ii) provide a named BT Project Manager who will be available to attend meetings at your Site depending on your location for the duration of the Initial Setup.
(d) **Custom Rule Design and Deployment**
(i) BT will provide you with the Standard Default Rule Set.
(ii) You will select three additional Custom Rules that you have agreed with BT when you place the Order and ensure that the Custom Rules you select meet your requirements. Any additional Custom Rules will be charged, in addition, on a time and materials basis.
(iii) If you have requested changes to your Custom Rules during the Controlled Deployment Custom Rules Optimisation Period, you will follow the Custom Rules Change Management Process set out in Paragraph 2.7.2.
(iv) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in the creation of your Custom Rules.
(v) Should BT elect to standardise a Custom Rule requested by you, the rule will be added to the Standard Default Rule Set, made available to BT's wider customer base, in which case the rule will cease to count towards your Custom Rules allocation and no additional Charges will apply. In such circumstances, BT will own the Intellectual Property Rights in relation to the rule.

(vi) Subject to receiving acceptable information from the External Data Sources, BT will configure the BT Cloud SIEM Service to implement the Custom Rules agreed with you and in accordance with Paragraph 8.2.

(vii) Unless otherwise set out in any applicable Order, the Custom Rule Design and Deployment activities set out in this Paragraph 2.4.1(d) will be undertaken remotely by BT.

(viii) The SOM will work with you in respect of the Custom Rule Design and Deployment.

(ix) BT may apply additional Charges if work cannot be undertaken remotely and BT is required to attend the Site(s).

(e) **Data Source Connection**

(i) BT will configure the BT Cloud SIEM Service to receive Event Log Data from the External Data Sources agreed with you and set out in the Data Capture Form attached to the applicable Order.

(ii) You will configure the External Data Sources to send Logs to the BT Cloud SIEM Service or provide BT with the requisite details and consents to enable BT to configure the External Data Sources directly, as set out in any applicable Order.

(iii) You will connect the External Data Sources to the BT Cloud SIEM Service unless BT provides the data source in which case BT will connect the External Data Source to the BT Cloud SIEM Service.

(iv) BT may at your request, connect additional External Data Sources, to the BT Cloud SIEM Service and this will be charged, in addition, on a time and material basis, unless otherwise set out in any applicable Order.

(v) BT will not be liable for any failure of the BT Cloud SIEM Service to process Logs sent to the BT Cloud SIEM Service from External Data Sources not set out in the Data Capture Form or otherwise set out in any applicable Order.

(vi) BT will only undertake threat correlation or threat monitoring from External Data Sources that are set out in the Data Capture Form.

(vii) BT may apply additional Charges if work cannot be undertaken remotely and requires BT to attend the Site(s).

2.4.2 **MS2**

(a) BT will provide you with access to the Security Portal for up to a maximum of five Users.

(b) BT will appoint a SOM to be your single point of contact during the Initial Setup and Controlled Deployment. The SOM will undertake any activity remotely and will not visit your Site.

(c) BT will provide you with access to a named SOM on a shared basis, for the duration of the Service, to assist with any issues or requests.

(d) You may request that BT, at an additional Charge, provides a named SOM who will be available to attend meetings at your Site depending on your location for the duration of the Initial Setup and Controlled Deployment.

(e) **Custom Rule Design and Deployment**

(i) You will select 15 additional Custom Rules that you have agreed with BT when you place the Order and ensure that the Custom Rules you select meet your requirements. Any additional Custom Rules will be charged, in addition, on a time and materials basis.

(ii) The SOM to assist you with the configuration of the BT Cloud SIEM Service in accordance with the agreed Custom Rules.

2.4.3 **MS3**

(a) BT will provide you with access to the Security Portal for up to a maximum of five Users.

(b) BT will provide a named SOM for the duration of the Initial Setup and Controlled Deployment.

(c) BT will provide you with access to a named SOM on a dedicated basis, for the duration of the Service, to assist with any issues or requests.

(d) **Custom Rule Design and Deployment**

(i) You will select 30 additional Custom Rules that you have agreed with BT when you place the Order and ensure that the Custom Rules you select meet your requirements. Any additional Custom Rules will be charged, in addition, on a time and materials basis.

(ii) You will provide a named contact and appropriate technical support to work with BT during the Controlled Deployment Custom Rules Optimisation Period.

(e) BT will provide further policies tailored to your specific requirements to use as your Custom Rules.

2.5 **Controlled Deployment**

BT will work with you during the Controlled Deployment Custom Rules Optimisation Period in accordance with the Managed Service Package selected by you, as follows:

2.5.1 **MS1**

(a) The provisions of Paragraph 9.2 will apply.
(b) BT will provide you with User Guides.
(c) You will comply with the User Guides.
(d) Both of us will direct all communication to the other via the SOM.
(e) If the Controlled Deployment Custom Rules Optimisation Period is extended for any reason beyond 90 days from the date you receive Notice from BT in accordance with Paragraph 8.2.2, BT may apply additional Charges.

2.5.2 **MS2 and MS3**

(a) **Customer Training**

(i) BT will deliver training, via Webex, for the maximum number of permitted concurrent Users as set out in Paragraph 2.4.1(a).
(ii) Additional training may be offered at BT's sole discretion.

(b) You may communicate with BT directly via the SOM or email.

2.6 **Monitoring and Management**

The Monitoring and Management will commence on the Service Start Date.

2.6.1 **MS1**

(a) **Proactive Monitoring**

(i) BT will monitor the performance of the BT Cloud SIEM Service at intervals set by BT and, where possible, provide advance warning to you through the Security Portal or via email of impending issues that may affect the BT Cloud SIEM Service and that BT identifies as a result of the monitoring. BT may not identify all impending issues.
(ii) You are responsible for resolving the issues that BT provides you advance warning of in Paragraph 2.6.1(a)(i).
(iii) You will ensure that you or third parties, as required, configure routing/permissions on platforms or Enabling Services to allow BT to carry out the monitoring.

(b) **Cloud SIEM Technical Incident Monitoring**

BT will:

(i) proactively monitor and manage the BT Cloud SIEM Service 24x7x365.

(c) **Cloud SIEM Upgrades**

(i) BT may from time to time upgrade any Software or firmware used to deliver the Service to ensure that they remain within the Supplier's supported software specification. The dates and times of any Software or firmware upgrades will be notified to you in advance.
(ii) You will confirm to BT any change in the number of devices/log sources you are adding in, to your Cloud SIEM Service.

(d) **Capacity Management**

(i) If BT identifies that changes in your usage volumes could result in the Service being unable to process the data effectively, or BT identifies that your usage volumes are higher than that agreed, BT will contact you to discuss any recommended changes to the data that is collected or change in Charges as a result of your increased usage.
(ii) If you do not agree to make changes to the data collected, following advice from BT in accordance with Paragraph 2.6.1(d)(i), BT will not be liable for any performance issues of the BT Cloud SIEM Service and will not be liable under any applicable Service Level.

(e) **Maintenance**

(i) BT will maintain the Software or firmware used to deliver the Service on a regular basis.

(f) **Technical Incident and Fault Management**

(i) You will notify all Technical Incidents to the SOM.
(ii) All communications with the Service Desk will be in English.
(iii) The Service Desk that will action the Technical Incident notifications is available 24x7x365 and is staffed by security trained professionals.
(iv) BT will give you a Ticket.
(v) BT will assess the Technical Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	Serious impact and Technical Incident cannot be circumvented, typically where the BT Cloud SIEM Service is completely down / unavailable; for example: your Site is isolated or there is a complete loss of service to a Site or critical business functions are prevented from operating.
P2	Large impact on a portion of the BT Cloud SIEM Service and cannot be circumvented, causes significant loss of the BT Cloud SIEM Service, but the impacted business function is not halted; for example: there is a complete loss of primary link and the BT backup link (if provided) is invoked or business functions are disrupted but not prevented from operating.
P3	Small impact on the BT Cloud SIEM Service or where a single User or component is affected and it causes some impact to your business; for example there is an intermittent or occasional disturbance which does not have a major impact on the BT Cloud SIEM Service or where a temporary work around has been provided.
P4	Minor or intermittent impact to a non-operational element of the BT Cloud SIEM Service; for example a temporary failure of reporting or billing.
P5	Incident has no direct impact on the BT Cloud SIEM Service. Records normally kept for Technical Incidents are used for information purposes. Example: to track upgrades, for planned outages or for enquiries as well as customer provoked Incidents.

(vi) BT will review the status of the Technical Incident and amend the priority level assigned initially if necessary.

(vii) BT will keep you informed throughout the course of the Technical Incident resolution at regular intervals by posting updates on the Security Portal or via automated e-mails to the Customer Contact in accordance with Paragraph 10.1.

(viii) BT will inform you when it believes the Technical Incident is cleared and will close the Ticket when:

(ix) you confirm that the Technical Incident is cleared within 24 hours after having been informed; or

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

(xi) If you confirm that the Technical 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 Technical Incident.

(xii) Where BT becomes aware of a Technical Incident, Paragraphs 2.6.1(f)(iv) to 2.6.1(f)(xi) will apply.

(g) **Missing Log Source Monitoring and Reporting**

(i) BT will notify you, as soon as possible, if one or more of your External Data Sources, fitted with a Silent Device Alarm, fails to forward Event Log Data to the BT Cloud SIEM Service.

(ii) BT will investigate the Technical Incident to determine if the Software or firmware collecting the data is working and functioning correctly. If the Software or firmware is functioning correctly, BT will advise you of the External Data Sources that have stopped forwarding and you will investigate and restart the forwarding of the Event Log Data to the Software or firmware delivering the Service.

(h) **Cloud Log Management**

(i) For the BT Cloud SIEM Delivery Model, as set out in Paragraph 2.3.1:

i. the default online retention for Log storage will be 90 days;

ii. you may search and view the last 31 days of Logs; and

iii. you may request via the SOM that Logs older than 31 days be made available for viewing and search.

(i) **Event Correlation**

(i) BT will correlate incoming Events and categorise each Event according to its severity for inspection by the BT SOC.
(ii) BT will correlate Events in accordance with the Standard Default Rule Set and the three Custom Rules selected by you and set out in any applicable Order.
(iii) BT may, at its sole discretion, agree to use additional Custom Rules in the correlation of Event Log Data, as set out in any applicable Order.
(iv) BT may apply additional Charges if you exceed the three Custom Rules.

(j) **Security Event Management**

BT will:

(i) analyse Event data generated by the Event Correlation engine;
(ii) assess appropriate actions to take; and
(iii) if necessary, alert you via email to any potential threats.

(k) **Reports**

(i) BT will provide you with reporting for the BT Cloud SIEM Service via the Security Portal in accordance with this Paragraph 2.6.1(k) or secure email,

(l) **Security Incident Management**

(i) **Case Registration**

i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
ii. BT will raise a Case for each Security Incident that is notified to you.

(ii) **Case and Security Incident Management**

Where a Case has been raised by BT in respect of any Security Incident, the BT SOC will contact your nominated customer service teams to notify them of the incident following which BT will close the Case. If your nominated customer service team does not take any necessary remedial action, BT is not responsible for the ongoing effects of the Security Incident.

2.6.2 **MS2**

(a) **Proactive Monitoring**

(i) Both of us will agree a process for BT to contact you when it identifies an issue that impacts the BT Cloud SIEM Service.

(ii) BT will use historic and current metrics captured via the monitoring of the BT Cloud SIEM Service to forecast issues that may impact the performance of the BT Cloud SIEM Service and make recommendations to you by e-mail, as agreed by you.

(b) **Technical Incident and Fault Management**

(i) You will notify all Technical Incidents to the Service Desk directly via email or via the Security Portal.
(ii) If you notify the Technical Incident to the Service Desk directly you will have the option of communicating in the languages agreed with BT. If the Service Desk is required to escalate the Technical Incident within BT or to a third-party vendor, then you may be required to communicate in English only.

(c) **Event Correlation**

(i) BT will correlate Events in accordance with the Standard Default Rule Set and the 15 Custom Rules selected by you and set out in any applicable order.
(ii) BT may apply additional Charges if you exceed the 15 Custom Rules.

(d) **Reports and Security Incident Management**

(i) **Case Registration**

i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
ii. Mitigation Planning: the SOM will provide you with guidance on preventing the recurrence of Security Incidents. This advice may include:
(a) advising on malware related to a botnet, known to use command and control servers, that your devices have attempted to connect to; and

(b) advising on blocking certain defined network traffic or specific Twitter feeds, at firewall, proxy, or other appropriate control point.

(ii) **Case and Security Incident Management**

Where a Case has been raised by BT in respect of any Security Incident, the BT SOC will contact your nominated customer service teams to:

i. advise of any necessary remedial action they need to take; and
ii. confirm that they have completed any necessary remedial action,

following which BT will close the Case. If your nominated customer service team does not take the necessary remedial action, BT is not responsible for the ongoing effects of the Security Incident.

2.6.3 **MS3**

(a) **Technical Incident and Fault Management**

(i) You will agree with BT whether you report Incidents directly to the Service Desk, via the Security Portal or to the regional BT SOC.

(b) **Event Correlation**

(i) BT will correlate Events in accordance with the Standard Default Rule Set and the 30 Custom Rules selected by you and set out in any applicable Order.
(ii) BT may apply additional Charges if you exceed the 30 Custom Rules.

(c) **Reports and Security Incident Management**

(i) **Case Registration**

i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
ii. The SOM will provide RCA Support and Ad Hoc Post Security Incident Activity Support in relation to all Priority 1 Security Incidents.

2.7 **Continuous Improvement**

2.7.1 **Reviews**

(a) **MS1**

(i) The SOM will carry out a review every two months per annum as follows:

i. a BT Cloud SIEM Service review, focussing on the performance of the BT Cloud SIEM Service.

(ii) The SOM will provide you with a report on the review via email or the Security Portal, as agreed between us.
(iii) If requested by you and if agreed to by BT, both of us may hold a conference call to discuss the report.
(iv) If BT has agreed to participate in a conference call you will ensure that any report the SOM provides you with will be reviewed by your suitably qualified personnel who are participating in the conference call prior to the conference call taking place.
(v) You will take appropriate action to address issues as recommended by the SOM:

i. in respect of the BT Cloud SIEM Service including implementing security improvements as agreed with the SOM or as advised by the SOM as your responsibility;

(b) **MS2**

(i) The SOM will carry out a review monthly as follows:

i. a BT Cloud SIEM Service review focussing on the performance of the BT Cloud SIEM Service against Service Levels and Service Targets;
ii. a review of the effectiveness of the Custom Rules applied to your BT Cloud SIEM Service and the need to fine tune or amend the Custom Rules; and

(ii) In addition to taking the action set out in Paragraph 2.7.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Rules as recommended by the SOM.

(c) **MS3**

(i) The SOM will carry out a review at intervals agreed by both of us but not less than monthly as follows:

i. a BT Cloud SIEM Service focussing on the performance of the BT Cloud SIEM Service against Service Levels and Service Targets;
ii. a review of the effectiveness of the Custom Rules applied to your BT Cloud SIEM Service and the need to fine tune or amend the Custom Rules; and
iii. The SOM will also carry out a six-monthly Security Posture review. The SOM will create an action plan with the aim of improving your Security Posture;

(ii) In addition to taking the action set out in Paragraph 2.7.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Rules as recommended by the SOM.

2.7.2 **Custom Rules Change Management Process**

(a) BT will implement changes to the Custom Rules in response to your request subject to the following process:

(i) the authorised Customer Contact will submit requests to change the Custom Rules via an email service request to the BT SOC or SOM, providing sufficient detail and clear instructions as to any changes required;
(ii) BT will check each request for its complexity and assess whether the change should be completed via the Custom Rules Change Management Process or whether it requires to proceed in accordance with Clause 31 (Service Amendment) of the General Terms;
(iii) only changes to Custom Rules will be completed via the Custom Rules Change Management Process; and
(iv) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in writing your change request.

(b) **MS1**

(i) BT will provide contact details for the BT SOC or SOM to all pre-agreed and authorised Customer Contacts to enable you to submit your change requests.
(ii) Simple Changes subject to the Reasonable Use Policy set out in Paragraph 2.7.2(b)(v) are included in the Charges.
(iii) Complex Change requests will proceed in accordance with Clause 31 (Service Amendment) of the General Terms and BT will charge you the cost of implementing Complex Changes.
(iv) BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change.
(v) BT will apply the following "reasonable use" restrictions ("**Reasonable Use Policy**") for changes to the Custom Rules:

i. you will not raise Standard Change requests more frequently than:
   a. six per month per Cloud SIEM Device in respect of MS1;
   b. eight per month per Cloud SIEM Device in respect of MS2; and
   c. 10 per month per Cloud SIEM Device in respect of MS3;
ii. you will not raise Urgent Change requests more frequently than:
   a. one per month per Cloud SIEM Device in respect of MS1;
   b. two per month per Cloud SIEM Device in respect of MS2; and
   c. three per month per Cloud SIEM Device in respect of MS3.
iii. where BT's measurements show that change requests are being raised more frequently than as set out in Paragraphs 2.7.2(b)(v)i and 2.7.2(b)(v)ii, BT may, either:
   a. 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
   b. review your requirements and agree with you an appropriate alternative implementation process and any associated charges.

(vi) BT will use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. BT may charge you the cost of implementing an Emergency Change.
(vii) BT may implement an Emergency Change without your approval.
(viii) You are deemed to have approved all changes to the Custom Rules that you submit to BT.
(ix) You are responsible for the impact of BT implementing the changes and BT is not liable for any consequences arising from the impact of the implementation of the changes.

(c) **MS2**

(i) The authorised Customer Contact may submit requests to modify the Custom Rules, via email to the SOC or direct to the SOM.

(d) **MS3**

(i) BT will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested Simple Changes and Complex Changes and advise you appropriately and will not be liable for any consequence arising from:

i. your miss-specification of your security requirements in relation to the Custom Rules; or

ii. unforeseen consequences of a correctly specified and correctly implemented Custom Rule.

3 Service Options

There are no Service Options available for the BT Cloud SIEM Service.

4 Service Management Boundary

4.1 BT will provide and manage the BT Cloud SIEM Service in accordance with Parts A, B and C of this Annex and as set out in any applicable Order ("**Service Management Boundary**").

4.2 BT will have no responsibility for the BT Cloud SIEM Service outside the Service Management Boundary.

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

4.4 **Service Restrictions**

4.4.1 BT will not be liable if BT is unable to deliver the BT Cloud SIEM Service, or any part of the BT Cloud SIEM Service, due to a failure of any Customer Equipment, including any Customer log sources.

4.4.2 BT does not guarantee that the BT Cloud SIEM Service will detect or block all malicious threats.

4.4.3 The BT Cloud SIEM Service assumes standard logs and functionality, as communicated to you by BT. BT will not be liable for any inability to provide the BT Cloud SIEM Service, or any degradation of the BT Cloud SIEM Service, if you do not have and maintain the appropriate logs and functionality.

5 Associated Services

5.1 You will have the following services in place that will connect to the BT Cloud SIEM Service and are necessary for the BT Cloud SIEM Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 a stable internet connection so that the BT Cloud Siem Service can communicate to the Cloud SIEM Devices platform,

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

5.2 If BT provides you with any services other than the BT Cloud SIEM Service, this Annex will not apply to those services and those services will be governed by their separate terms.

6 Equipment

6.1 **BT Equipment**

6.1.1 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.

6.1.2 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.

6.2 **Use of BT Equipment**

In relation to BT Equipment, you will:

6.2.1 keep the BT Equipment safe and without risk to health;

6.2.2 only use the BT Equipment, or allow it to be used, in accordance with any instructions or authorisation BT may give and for the purpose for which it is designed;

6.2.3 not move the BT Equipment or any part of it from the Site(s) without BT's written consent and, you will pay BT's costs and expenses reasonably incurred as a result of such move or relocation;

6.2.4 not make any alterations or attachments to, or otherwise interfere with, the BT Equipment, nor permit any person (other than a person authorised by BT) to do so, without BT's prior written consent and, if BT gives its consent, agree that any alterations or attachments are part of the BT Equipment;

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

6.2.6 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;

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

6.2.8 obtain appropriate insurance against any damage to or theft or loss of the BT Equipment;

6.2.9 in addition to any other rights that BT may have, reimburse BT for any losses, costs or liabilities arising from your use or misuse of the BT Equipment or where the BT Equipment is damaged, stolen or lost, except where the loss or damage to BT Equipment is a result of fair wear and tear or caused by BT;

6.2.10 ensure that the BT Equipment appears in BT's name in your accounting books;

6.2.11 where there is a threatened seizure of the BT Equipment, or an Insolvency Event applies to you, immediately provide BT with Notice so that BT may take action to repossess the BT Equipment; and

6.2.12 notify any interested third parties that BT owns the BT Equipment.

6.3 **Sale of Goods**

The UN Convention on Contracts for the International Sale of Goods will not apply to the Contract.

7 Specific Terms

7.1 **Changes to the Contract**

7.1.1 BT may propose changes to this Annex or the Charges (or both) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

7.1.2 Within 21 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

7.1.3 If we have not reached agreement in accordance with Paragraph 7.1.2(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Annex will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 7.1.2(c) or BT may give Notice of termination, in which case BT will cease delivering the BT Cloud SIEM Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.2 **Customer Committed Date**

7.2.1 If you request a change to the BT Cloud SIEM Service or any part of the BT Cloud SIEM Service, then BT may revise the Customer Committed Date to accommodate that change.

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

7.3 **Licence**

BT gives you a non-exclusive, non-transferable and limited right to use the BT Cloud SIEM Service for your internal business purposes only.

7.4 **Invoicing**

7.4.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:

(a) Installation Charges, in advance once you have placed the Order;

(b) Recurring Charges, monthly in arrears (depending on your billing frequency). Note that for any period where the BT Cloud SIEM Service is provided for less than one month, the full monthly charge will be applied;

(c) Professional Services Charges.

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

(a) Charges for investigating Technical Incidents that you report to BT where BT finds no Technical Incident or that the Technical Incident is caused by something for which BT is not responsible under the Contract;
(b) Charges for expediting provision of the BT Cloud SIEM Service at your request after BT has informed you of the Customer Committed Date;
(c) additional Charges in accordance with Paragraph 2.5.1(e) if the Controlled Deployment Custom Rules Optimisation Period is extended for any reason beyond 90 days Business Days after receiving Notice from BT in accordance with Paragraph 8.2.2;
(d) Charges for appointing and providing a named SOM if you have purchased MS1 OR MS2 in accordance with Paragraphs 2.4.1(b) or 2.4.2(b) as applicable;
(e) Charges for additional Custom Rules in accordance with Paragraphs 2.4.1(d)(ii), 2.4.2(e)(i) and 2.4.3(d)(i);
(f) Charges for supporting new non-standard log sources;
(g) Charges for the cost of implementing Complex Changes in accordance with Paragraph 2.7.2(b)(iii) and Emergency Changes in accordance with Paragraph 2.7.2(b)(vi);
(h) Charges associated with an appropriate alternative implementation process if you have raised change requests more frequently than allowed by the Reasonable Use Policy in accordance with Paragraph 2.7.2(b)(v)iii;
(i) Charges to cover any costs reasonably incurred by BT as a result of any non-conformity of the Customer Equipment in accordance with Paragraph 9.1.18;
(j) any other Charges as set out in any applicable Order or as otherwise agreed between both of us; and
(k) any Termination Charges incurred in accordance with Paragraph 7.5 upon termination of the relevant BT Cloud SIEM Service.

7.4.3 **Usage Volume Reasonable Use Policy**

(a) Where your monthly usage volume exceeds the agreed Usage Volume, as determined by the average usage volume measured over a consecutive three-month period, BT reserves the right to increase the monthly Charges to reflect the increase in usage volumes.
(b) BT will notify you at least one month in advance before any changes in the Charges are applied.

7.5 **Termination Charges**

7.5.1 If you terminate the Contract or the BT Cloud SIEM Service for convenience in accordance with Clause 17 of the General Terms you will pay BT:

(a) all outstanding Charges or payments due and payable under the Contract;
(b) any remaining Charges outstanding with regard to BT Equipment;
(c) any other Charges as set out in any applicable Order; and
(d) any charges that BT has to pay a supplier as a result of early termination of the BT Cloud SIEM Service.

7.5.2 In addition to the Charges set out at Paragraph 7.5.1 above, if you terminate during the Minimum Period of Service or any Renewal Period, you will pay BT:

(a) for any parts of the BT Cloud SIEM Service that were terminated during the first 12 months of the Minimum Period of Service or Renewal Period, Termination Charges, as compensation, equal to:
(i) 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service;
(ii) 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service or Renewal Period;
(iii) any waived Installation Charges; and
(b) for any parts of the BT Cloud SIEM Service that were terminated after the first 12 months of the Minimum Period of Service or during a Renewal Period, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service or the Renewal Period.

7.6 **Upgrade to a Higher Managed Service Package**

7.6.1 You may upgrade to a higher Managed Service Package during the Minimum Period of Service.

7.6.2 No Termination Charges will be payable from the Managed Service Package you are moving from. New Charges for the upgraded Managed Service Package will be set out in the Order.

7.6.3 A new Minimum Period of Service will apply to the upgraded Managed Service Package as set out in the Order.

7.6.4 If you upgrade to a higher Managed Service Package under either this Annex, the Schedule or any other Associated Service, you must upgrade your entire Contract to that higher Managed Service Package.

7.6.5 You cannot downgrade to a lower Managed Service Package.

7.7 **Amendments to the Managed Service Schedule**

7.7.1 Paragraphs, 2.5 (**Maintenance Care Levels**), 2.7 (**Vital Port Monitoring**), 2.8 (**In-Band and Out of Band Management**), 2.9 (**Configuration Management**) and 2.10 (**Software Upgrades**) of the Schedule will not apply.

7.7.2 Paragraph 2.11.3 (**Network Reporting**), 2.11.4 (**IPSLA Reporting**) and 2.11.5 (**Application Reporting**) of the Schedule will not apply.

7.7.3 Paragraph 2.11.6 (**Vendor Network and Application Reporting**) of the Schedule will not apply if you have selected the MS1 Package but if you have selected either the MS2 or MS3 Package, your reports will be generated by the SOM.

7.7.4 Paragraph 2.12 (**Capacity Management**) and 2.13 (**Availability Management**) of the Schedule will not apply.

7.7.5 Paragraph 2.16.5 (**WLAN Survey**), 2.16.6 (**Network Assessment Physical Detail Collection Package and Network Assessment Physical Detail Collection Day Rate**), 2.16.7 (**Infrastructure Cabling**) and 2.16.8 (**PDS Installation Services**) of the Schedule will not apply.

7.7.6 The wording of Paragraph 4.1 (**Changes to the Contract**) of the Schedule is deleted and replaced with the following:

4.1.1 BT may propose changes to this Schedule, the General Terms or the Charges (or any of them) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

4.1.2 Within 10 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

4.1.3 If we have not reached agreement in accordance with Paragraph 4.1.2(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Schedule will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 4.1.2(c) or BT may give Notice of termination, in which case BT will cease delivering the BT Cloud SIEM Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.7.7 Regardless of what it may say in Paragraph 4.2 (**Minimum Period of Service and Renewal Periods**) of the Schedule:

4.2.1 You may request an extension to the BT Cloud SIEM Service for a Renewal Period by Notice in writing to BT at least 90 days before the end of the Minimum Period of Service or Renewal Period ("**Notice of Renewal**").

4.2.2 If you issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will extend the BT Cloud SIEM Service for the Renewal Period and both of us will continue to perform each of our obligations in accordance with the Contract.

4.2.3 If you do not issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will cease delivering the BT Cloud SIEM Service at the time of 23:59 on the last day of the Minimum Period of Service or Renewal Period.

4.2.4 If the BT Cloud SIEM Service is the only Associated Service purchased under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will not apply to the Managed Service and Paragraph 7.7.7 of this Annex will apply; and

7.7.8 4.2.5 If the BT Cloud SIEM Service is purchased along with other Associated Services under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will apply to the Managed Service and the other Associated Services and Paragraph 7.7.7 of this Annex will apply only to the BT Cloud SIEM Service.

7.7.9 Regardless of what it may say in Paragraphs 4.3.2 and 4.3.3 of the Schedule, if either of us terminates the Managed Service in accordance with Paragraph 4.3.1 of the Schedule, the BT Cloud SIEM Service will automatically terminate at the same time and you will pay Termination Charges in accordance with Paragraph 4.7 of the Schedule as amended by this Annex.

7.7.10 Paragraph 4.10 (**Security**) of the Schedule will not apply.

7.7.11 Paragraphs 5.1.3 (**BT obligations for PDS Installation**) and 5.3 (**BT's obligations During Operation**) of the Schedule will not apply.

7.7.12 Paragraphs 6.1.4 (**providing BT access to any of your Sites**), 6.1.6 (**specialist equipment at your Site**), 6.1.9 (**LAN protocols and applications compatible with the Managed Service and Associated Service**) and 6.2.13 (**your obligations on expiry or termination of the Managed Service**) of the Schedule will not apply.

7.7.13 Paragraphs 6.3 (**UCC Obligations**), 6.4 (**WAN Obligations**) and 6.5 (**LAN Obligations**) of the Schedule will not apply.

7.7.14 The wording in Paragraph 7 (**Notification of Incidents**) of the Schedule is deleted and replaced with the following:

7.1 Where you become aware of an Incident or a Security Incident:

7.1.1 The Customer Contact will report it to the Service Desk;

7.1.2 BT will give you a Ticket;

7.1.3 BT will inform you when it believes the Incident or Security Incident is cleared and will close the Ticket when:

(a) you confirm that the Incident or Security Incident is cleared within 24 hours after having been informed; or

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

7.1.4 If you confirm that the Incident or Security 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 or Security Incident.

7.1.5 Where BT becomes aware of an Incident or Security Incident, Paragraphs 7.1.2, 7.13 and 7.1.4 as amended by Paragraph 7.7.14 of this Annex will apply.

7.1.6 This Paragraph 7 will not apply to Security Incidents if you have selected the MS1 Package.

7.7.15 Part C (**Service Levels**) of the Schedule will be deleted and Part C of this Annex will apply instead.

Part B – Service Delivery and Management

BT's Obligations

8.1 **Service Delivery**

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

8.1.1 will, once the requirements of the BT Cloud SIEM Service have been confirmed and agreed, and, where applicable, you provide the details set out in Paragraph 7.2.1, provide you with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date;

8.1.2 will not be responsible for any:

(a) delay in providing;
(b) interruption to; or
(c) degradation of,

the BT Cloud SIEM Service caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the BT Cloud SIEM Service, or any actions taken by BT at your direction.

8.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

8.2.1 conduct a series of standard tests on the BT Cloud SIEM Service to ensure that it is configured correctly; and

8.2.2 on the date that BT has completed the activities in this Paragraph 8.2, confirm that the Cloud SIEM Service is available for Controlled Deployment Custom Rules Optimisation and performance of any Acceptance Tests in accordance with Paragraph 9.2.

8.3 **During Operation**

On and from the Service Start Date, BT:

8.3.1 will respond and use reasonable endeavours to remedy a Technical Incident without undue delay if BT detects or if you report a Technical Incident;

8.3.2 will respond to Security Incidents as set out in Paragraph 10.4;

8.3.3 will maintain and use reasonable endeavours to provide uninterrupted access to all pre-agreed and authorised Customer Contacts to the Security Portal but BT does not guarantee that the Security Portal will be available at all times or will be fault free;

8.3.4 will retain normalised Event Log Data as follows:

(a) 30 Business Days of detailed information and Event Log Data online; and
(b) 60 days offline;

8.3.5 may, in the event of a security breach affecting the BT Cloud SIEM Service, require you to change any or all of your passwords;

8.3.6 may install additional BT Equipment on your Site, for the purpose of monitoring and management of the BT Cloud SIEM Service;

8.3.7 will use secure protocols or provide a secure management link to connect to the Software or firmware at your Site(s) via the Internet or other agreed network connection, in order to monitor the BT Cloud SIEM Service proactively and to assist in Technical Incident diagnosis; and

8.3.8 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the BT Cloud SIEM Service. However, BT may inform you with less notice than normal where Maintenance is required in an emergency. BT may carry out the Maintenance remotely or by visiting the Site as appropriate.

8.4 **The End of the Service**

On termination of the BT Cloud SIEM Service by either of us, BT:

8.4.1 will provide configuration information relating to the BT Cloud SIEM Service provided at the Site(s) in a format that BT reasonably specifies;

8.4.2 may disconnect and remove any BT Equipment located at the Site(s); and

8.4.3 may delete any Content, including stored Logs or any configuration data relating to BT's management of the BT Cloud SIEM Service.

9 Your Obligations

9.1 **Service Delivery**

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

9.1.1 provide BT with the names and contact details of the Customer Contact including escalation details, but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;

9.1.2 nominate suitably empowered and informed customer service teams that will interact with the BT SOC when raising Technical Incidents and when responding to Security Incidents;

9.1.3 provide BT with information reasonably requested (including business and technical information accurate in all respects) in a timely manner and promptly notify BT, in writing, of any changes to the information you have provided;

9.1.4 provide BT with a copy of your security policies;

9.1.5 ensure that you have the capabilities, Log Forwarders and supported protocols in place to be able to forward Event Log Data to the relevant Cloud SIEM Software or firmware;

9.1.6 provide BT with the ability to install any Cloud SIEM Software or firmware inside your network on a network segment where Customer Equipment Log data sources being monitored can deliver Event Log Data to the Cloud SIEM Service;

9.1.7 attend integration meetings to discuss further tuning and configuration of the Cloud SIEM Service;

9.1.8 complete any preparation activities including installation and maintenance of any software or hardware that is not included as part of the BT Cloud SIEM Service, that BT may request to enable you to receive the BT Cloud SIEM Service promptly and in accordance with any reasonable timescales;

9.1.9 where applicable, you will prepare and maintain the Site(s) for the supply of the BT Cloud SIEM Service, in accordance with any instructions from BT, including:

(a) complying with any Site accommodation requirements as set out in any applicable Order;

(b) providing a secure, continuous power supply at the Site(s) for the operation and maintenance of the BT Cloud SIEM Service at such points and with such connections as BT specifies, and, in order to mitigate any interruption to the BT Cloud SIEM Service resulting from failure in the principal power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards.

9.1.10 give Notice to BT, five Business Days in advance, and provide details, of any changes to your network, that may affect the functioning of the BT Cloud SIEM Service. If this information is not provided, or is provided less than five Business Days before a change, then BT will not be liable for any Technical or Security Incidents or incorrect functioning of the BT Cloud SIEM Service as a result of the change;

9.1.11 only use any Cloud SIEM Hardware Sentry, or allow it to be used, in accordance with any instructions or authorisation BT may give and for the purpose for which it is designed;

9.1.12 not relocate any Cloud SIEM Hardware Sentries without BT's prior written consent;

9.1.13 ensure that your WAN or Internet access circuit bandwidth is sufficient to meet your requirements and for the management access by BT;

9.1.14 manage, and provide BT with, accurate details of your internal IP Address design;

9.1.15 ensure that the Cloud SIEM Devices 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 if BT has agreed to provide any part of the BT Cloud SIEM Service using Customer Equipment, ensure that the relevant Customer Equipment:

(a) complies with any minimum specification given to you by BT;

(b) will comply with the requirements of Paragraph 9.3.4;

(c) is fully functional; and

if the relevant Customer Equipment does not comply with this Paragraph 9.1.16 then BT may raise an additional Charge to cover any costs reasonably incurred by BT as a result of the non-conformity, and any agreed installation dates and the Customer Committed Date(s) may no longer apply;

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

9.1.18 for any Customer Equipment used in the BT Cloud SIEM Service, be responsible for ensuring compliance with Applicable Law, including obtaining (if required) import and User licenses and the written authority from all respective authorities, and not act to misuse the BT Cloud SIEM 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 BT Cloud SIEM Service and BT may refuse to restore the BT Cloud SIEM Service until BT receives an acceptable assurance from you that there will be no further contravention; or

(b) terminate the BT Cloud SIEM Service upon Notice in accordance with Clause 18 of the General Terms;

9.1.19 provide BT with any information that is reasonably requested by any regulatory body, legal authority or government entity in any country in connection with regulatory, administrative, legal or lawful interception requests; and

9.1.20 be responsible for any issues on Users' machines or your servers (e.g. operating system, coding languages and security settings) making sure all issues are dealt with in a timely manner and ensure that any repaired devices are configured correctly to send data to the BT Cloud SIEM Service;

9.1.21 ensure that your network or Internet connectivity performs correctly and will send Logs to the Cloud SIEM Devices;

9.1.22 where you are providing the Customer Equipment on which the Virtual Cloud SIEM Device(s) are installed:

(a) provide the underpinning operating system on the Customer Equipment as well as the licencing and support agreements, including their renewal;

(b) upgrade the firmware of the Customer Equipment and your underpinning operating system software on which the Virtual Cloud SIEM Device is installed; and

9.1.23 ensure that all data provided to BT's technical design team is accurate to ensure that (if applicable) your HAC has the capacity to handle the full load independently.

9.2 **Controlled Deployment Custom Rules Optimisation and Acceptance Tests**

9.2.1 You will carry out the Controlled Deployment Custom Rules Optimisation within the Controlled Deployment Custom Rules Optimisation Period.

9.2.2 In respect of MS2 and MS3, both of us will jointly carry out the Controlled Deployment Custom Rules Optimisation. You will use reasonable endeavours to complete the Controlled Deployment Custom Rules Optimisation as early into the Controlled Deployment Custom Rules Optimisation Period as possible.

9.2.3 You will submit any changes you require to the Custom Rules as a result of the Controlled Deployment Custom Rules Optimisation through the Custom Rules Change Management Process.

9.2.4 You will carry out the Acceptance Tests for the BT Cloud SIEM Service during the Controlled Deployment Custom Rules Optimisation Period and use reasonable endeavours to complete the Acceptance Tests as early into the Controlled Deployment Custom Rules Optimisation Period as possible.

9.2.5 The BT Cloud SIEM Service is accepted by you if you confirm acceptance in writing during the Controlled Deployment Custom Rules Optimisation Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Controlled Deployment Custom Rules Optimisation Period.

9.2.6 Subject to Paragraph 9.2.7, the Service Start Date will be the earlier of the following:

(a) the date that you confirm or BT deems acceptance of the BT Cloud SIEM Service in writing in accordance with Paragraph 9.2.5; or

(b) the date of the first day following the Controlled Deployment Custom Rules Optimisation Period.

9.2.7 If, during the Controlled Deployment Custom Rules Optimisation Period, you provide BT Notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide you Notice that BT has remedied the non-conformance and inform you of the Service Start Date.

9.3 **During Operation**

On and from the Service Start Date, you will:

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

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

9.3.3 monitor and maintain any Customer Equipment connected to the BT Cloud SIEM Service or used in connection with the BT Cloud SIEM Service;

9.3.4 ensure that any Customer Equipment that is connected to the BT Cloud SIEM Service or that you use, directly or indirectly, in relation to the BT Cloud SIEM Service is connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;

9.3.5 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment does not meet any relevant instructions, standards or Applicable Law and redress the issues with the Customer Equipment prior to reconnection to the BT Cloud SIEM Service;

9.3.6 submit a request to BT if you want to change any Cloud SIEM Device's IP Address or change, add or remove any External Data Source;

9.3.7 notify BT of any planned work that you intend to undertake that may cause a Technical Incident;

9.3.8 ensure that all Enabling Services are maintained throughout the provision of the BT Cloud SIEM Service;

9.3.9 be responsible for any conclusions drawn from, and rectification of, any issues identified by use of the BT Cloud SIEM Service, supported by BT in accordance with the Service Level selected by you and set out in any applicable Order;

9.3.10 maintain a written list of current Security Portal Users and provide a copy of such list to BT within five Business Days following BT's written request at any time;

9.3.11 in respect of the BT Cloud SIEM Service:

(a) ensure that appropriate Log level auditing is turned on for all data sources monitored by the Cloud SIEM Devices. If the Log level auditing is not turned on, this will impact the BT Cloud SIEM Service;

(b) attend review meetings, as required by BT;

(c) prior to the meeting referred to in Paragraph 9.3.11(b), provide the most up to date network diagram of your existing IT network; and

(d) if you fail to attend the review meetings regularly, BT has the right to refuse your requests for tuning the BT Cloud SIEM Service; and

9.3.12 in the event of a Technical Incident requiring your technical support, you will provide BT with the necessary support and timely authorisation for any necessary changes notified by BT to your Customer Contact.

9.3.13 Provide 60 days' notice prior to termination, if you require your Logs to be transferred.

9.4 **The End of the Service**

On termination of the BT Cloud SIEM Service by either of us, you will:

9.4.1 provide BT with all reasonable assistance necessary to remove BT Equipment from the Site(s);

9.4.2 disconnect any Customer Equipment from BT Equipment located at the Site(s);

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 located at the Site(s) to be returned to BT or, if BT has elected to disconnect and remove the BT Equipment located at the Site(s) in accordance with Paragraph 8.4.2 above, arrange access for BT to carry out such disconnection and removal; and

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

Part C – Service Levels

10 Service Levels and Service Remediation Advice Targets

10.1 **Service Targets Technical Incident Management**

Priority	Target Progress Update		Target Time for Remediation Advice
	MS1	**MS2 and 3**	**MS1, 2 and 3**
P1	whenever a progress update is available	within 30 minutes	within 4 hours
P2	whenever a progress update is available	within 2 hours	within 8 hours
P3	whenever a progress update is available	within 4 hours	within 24 hours
P4	whenever a progress update is available	within 5 hours	within 72 hours
P5	whenever a progress update is available	within 6 hours	N/A

10.1.1 BT will aim to provide you with an initial response and remediation advice in relation to an Incident in accordance with the table above.

10.1.2 BT will not provide a progress update while BT is waiting on your input or feedback.

10.1.3 BT will not provide a Target time for Technical Incident resolution because the mitigation responsibility rests with you.

10.1.4 The Target Response Time and Target Time for Remediation Advice times shown in the table above are targets only and BT will have no liability for failure to meet them.

10.2 **Service Availability**

10.2.1 **Availability Service Level**

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

(b) You may request Availability Service Credits for Priority 1 Technical Incidents at the Standard Availability Service Credit Rate, as set out in Paragraph 10.3.4.

(c) The following table sets out the Availability Annual Targets, the Maximum Annual Availability Downtime, the Maximum Monthly Availability Target, the Standard Availability Service Credit Rate, and the Service Credit Interval for the applicable SLA Category:

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Target	Standard Availability Service Credit Rate	Service Credit Interval
Cat A	≥ 99.9%	4 hours	0 minutes	1.5%	1 hour

10.3 Availability Service Credits

10.3.1 If a Priority 1 Technical Incident occurs, BT will measure the Availability Downtime starting from when you report a Qualifying Technical Incident and ending when BT closes the Technical Incident in accordance with Paragraph 2.6.1(f)(viii).

10.3.2 BT will measure the Availability Downtime in units of full minutes during the Local Contracted Business Hours or during Contracted Maintenance Hours as applicable.

10.3.3 BT will then calculate the cumulative Availability Downtime for the calendar months in which the Priority 1 Technical Incident occurred ("**Cumulative Monthly Availability Downtime**").

10.3.4 If the Cumulative Monthly Availability Downtime of the BT Cloud SIEM Service exceeds the Maximum Monthly Availability Target, you may request Availability Service Credits for each Service Credit Interval of 1.5 per cent of the Monthly Recurring Charges for the relevant BT Cloud SIEM Service.

10.3.5 Service Availability Targets and Service Credits apply exclusively to those areas of the Service over which BT has control, including Virtual Sentry in the customers Cloud Infrastructure. Any failure to achieve an Availability Target as a result of faults or failures of your infrastructure (virtual or physical) will not attract any Service Credits.

10.3.6 You may request applicable Availability Service Credits in accordance with Paragraph 10.3.4 within 28 days of the end of the calendar month in which a Qualifying Priority 1 Technical Incident occurred, by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 10.3.6 will constitute a waiver of any claim for Service Credits for that calendar month.

10.3.7 Upon receipt of a valid request for Availability Service Credits in accordance with Paragraph 10.3.6:

(i) 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

(ii) 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.

10.3.8 Availability Service Credits will be aggregated and are available up to a maximum amount equal to three per cent (3%) of the monthly Recurring Charge for the affected BT Cloud SIEM Service.

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

10.3.10 The Service Levels under this Annex will not apply:

(i) in the event that Clause 8 or Clause 23 of the General Terms applies;

(ii) during any trial period of the BT Cloud SIEM Service;

(iii) where Availability is impacted due to any connections or cabling to the Cloud SIEM Devices; or

(iv) where Availability is impacted due to faults in your infrastructure (both physical and virtual) or third-party network.

10.4 **Security Incident Notification – Target Response Times**

10.4.1 From the Service Start Date, BT will aim to notify you in response to a Security Incident ("**Security Incident Notification**") in accordance with the target response times as set out in the table below for the Managed Service Package selected by you and set out in any applicable Order. A Security Incident Notification may take the form of a Security Event Classification Notification or a Security Case Assessment Notification, the applicable target response times for both are, set out in the table below.

10.4.2 No Service Credits apply to the provision of the Security Incident Notification target response times.

		Security Event Classification Notification Target			Security Case Assessment Notification Target		
BT Priority	**Managed Service Package**						
P1	MS1	30 minutes	✉		4 hours	✉	
	MS2	30 minutes	✉	☎	4 hours	✉	☎
	MS3	30 minutes	✉	☎	4 hours	✉	☎
P2	MS1	2 hours	✉		8 hours	✉	
	MS2	2 hours	✉		8 hours	✉	
	MS3	2 hours	✉	☎	8 hours	✉	☎
P3	MS1	4 hours	✉		24 hours	✉	
	MS2	4 hours	✉		24 hours	✉	
	MS3	4 hours	✉	☎	24 hours	✉	☎
P4	MS1	Weekly/Monthly in agreed reporting	✉		Weekly/Monthly in agreed reporting	✉	
	MS2	Weekly/Monthly in agreed reporting	✉		Weekly/Monthly in agreed reporting	✉	
	MS3	Weekly/Monthly in agreed reporting	✉		Weekly/Monthly in agreed reporting	✉	

Part D – Defined Terms

4 Defined Terms

In addition to the defined terms in the General Terms and the Schedule, capitalised terms in this Annex will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms and the Schedule, these defined terms will take precedence for the purposes of this Annex). BT has repeated some definitions in this Annex that are already defined in the General Terms and the Schedule. This is to make it easier for you to find the definitions when reading this Annex.

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the BT Cloud SIEM Service and that the BT Cloud SIEM Service is ready for use save for any minor non-conformities that will be resolved as a Technical Incident in accordance with Paragraph 8.3.1.

"**Ad Hoc Post Security Incident Activity Support**" means ad hoc activity, requested by you, following a previously reported Security Incident.

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

"**Availability Annual Target**" has the meaning given in the table at Paragraph 10.2.1 for the relevant SLA Category.

"**Availability Downtime**" means the period of time during which a Priority 1 Technical Incident exists as measured by BT in accordance with Paragraph 10.3.1.

"**Availability Service Credit**" means the Service Credit available for a failure to meet the Availability Service Level, as set out in Paragraph 10.3.1.

"**Availability Service Level**" has the meaning given in in Paragraph 10.2.1.

"**BT Cloud SIEM Delivery Model**" means the Delivery Model set out in Paragraph 2.3.1.

"**BT Cloud SIEM Service**" means has the meaning given in Paragraph 1.

"**BT Project Manager**" means the delivery manager BT appoints to liaise with you on Initial Setup and Controlled Deployment matters as set out in this Annex.

"**BT SOC**" means BT's security operations centre where BT's team of security analysts and specialists use various security technologies, to monitor and protect people, processes and assets across an organisation.

"**BT SOM**" or "**SOM**" means the security operations manager BT appoints to be the Customer's point of contact for the duration of the Service.

"**BT Virtual Sentry**" means the BT proprietarily owned software image that is issued to you by BT that you will install on your own virtual machine which will perform the same functionality as a Hardware Sentry.

"**Case**" means an issue that is "opened" and "closed" over a period of time to achieve resolution of a Security Incident that has been identified by the BT Cloud SIEM Service.

"**Cloud Infrastructure**" means the components needed for cloud computing, which includes hardware, abstracted resources, storage, and network resources. This can be hosted in public datacentres or your own datacentre.

"**Cloud Log Management**" means a feature of the BT Cloud SIEM Delivery Model provided by BT that can be used to store Log management data for up to 90 days.

"**Cloud SIEM Devices**" means a device and/or software and/or software platform used to process the Event Log Data.

"**Complex Change**" means a change that is not a Simple Change. Examples of Complex Changes are set out in the document titled Simple and Complex Changes which can be accessed through the Security Portal.

"**Continuous Improvement**" means the continuous improvement phase of the BT Cloud SIEM Service as set out in Paragraph 2.7.

"**Contracted Maintenance Hours**" means the times during which BT will provide maintenance for BT Equipment, which are Business Hours unless set out otherwise in any applicable Order.

"**Controlled Deployment**" means the controlled deployment phase of the BT Cloud SIEM Service as set out in Paragraph 2.5.

"**Controlled Deployment Custom Rules Optimisation**" means the fine tuning of your Custom Rules, conducted by you or in respect of Managed Service 2 or 3 only both of us jointly.

"Controlled Deployment Custom Rules Optimisation Period" means up to 90 Business Days after receiving Notice from BT in accordance with Paragraph 8.2.2. This period may be extended depending on various parameters including number of Logs, creation of rule sets and wider activities running and testing associated Playbooks.

"**Correlation Rules**" means a list of actions or event steps that specifically define the interaction between a role and a system to achieve a goal.

"**CPU**" means Central Processing Unit.

"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 10.3.3.

"**Custom Rules**" means bespoke Correlation Rules, specific to your requirements and individual deployment, that are created in the BT Cloud SIEM Service and set out in the applicable Order.

"**Custom Rules Change Management Process**" means the process in relation to changes to the Custom Rules as set out in Paragraph 2.7.2.
"**Custom Rule Design and Deployment**" means the Custom Rule design and deployment services set out in Paragraph 2.4.1(d).
"**Customer Service Description**" means the document that is available via the Security Portal and describes the BT Cloud SIEM Service and includes, for instance, the Standard Default Rule Set. This document is not legally binding.
"**Data Capture Form**" means the data capture form attached to an applicable Order in accordance with Paragraph 2.4.1(e)(i).
"**Delivery Model**" means the BT Cloud SIEM Delivery Model.
"**Emergency Change**" means 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 Priority 1 Technical Incident or a Priority 1 Security Incident.
"**EPS**" means events per second
"**EU**" means European Union.
"**Event**" means an event that is generated by your network, security or IT systems that is then forwarded to the BT Cloud SIEM Service for processing, analysis and storage.
"Event Correlation" means immediate analysis of normalised Event Log Data, to track threats, monitor User activity and track related transactions and data access and categorise each Event according to its severity for inspection by the BT SOC.
"**Event Log Data**" means the data that is generated by your network, security or IT system in response to events or activity on the External Data Sources.
"**External Data Sources**" means data from network and security devices and host systems that are compatible with the Supported Device List.
"**HAC**" means a high availability console, which is a platform that allows administrators comprehensive information on their primary and standby devices or databases.
"**Hardware Sentry**" means the hardware data collection appliances used when the BT Cloud SIEM Delivery Model has been selected by you.
"**Initial Setup**" means the facilitation of the setup and delivery of the BT Cloud SIEM Service as set out in Paragraph 2.4.
"**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 Contracted Business Hours**" means the times during which maintenance of any Access Line is provided, which are Business Hours unless set out otherwise in any applicable Order.
"**Log**" means an automatically produced and time-stamped file documenting events relevant to a particular program.
"**Log Forwarder**" means a software tool designed to collect event logs from one or more Cloud SIEM Devices and relay them to an intended destination. Log Forwarders are often used to translate Log messages from one format or protocol to another.
"**MAC Address**" means a hardware identification number that uniquely identifies each device on a network.
"**Managed Service Package"** means Managed Service 1, 2 and 3.
"**Managed Service 1**" or **"MS1"** means the Managed Service 1 Package as set out in this Annex.
"**Managed Service 2**" or **"MS2"** means the Managed Service 2 Package as set out in this Annex.
"**Managed Service 3"** or "**MS3"** means the Managed Service 3 Package as set out in this Annex.
"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 10.2.1(c) for the relevant SLA Category.
"**Maximum Monthly Availability Target**" has the meaning given in the table at Paragraph 10.2.1(c) for the relevant SLA Category.
"**Monitoring and Management**" means the monitoring and management phase of the BT Cloud SIEM Service as set out in Paragraph 2.6.
"**Monthly Recurring Charges**" means the monthly Recurring Charges for the BT Cloud SIEM Service for the three full previous months divided by three.
"**Notice to Amend**" has the meaning given in Paragraph 7.1.1.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**Playbooks**" means a collection of procedures that can be executed once a Security Incident is detected to contain the effects of the Security Incident and restore service.
"**Priority 1 Security Incident**" means actionable, high risk events or policy violations that have the potential to cause severe damage or disruption to your environment.
"**Priority 1 Technical Incident**" means a critical business impacting problem or issue, where no workaround exists. Examples include but are not limited to: Critical Services are not recoverable; Large number of users affected

and/or can't continue their job/role; Strategic Information has been compromised (confidentiality, availability, integrity); High Financial & Business Reputation Impact; Legal Requirements require an immediate response.

"**Priority 2 Technical Incident**" means a business impacting issue where a workaround exists. Examples include but are not limited to: Some critical Services are affected; a moderate number of users affected and/or can't continue their job/role adequately; non-strategic information has been compromised (confidentiality, availability, integrity); medium financial and business reputation impact.

"**Priority 3 Technical Incident**" means no critical Services are affected but they are degraded. Examples include but are not limited to: a minimum number of users affected and/or user impact is minor; no information has been compromised (confidentiality, availability, integrity); low financial and business reputation impact.

"**Priority 4 Technical Incident**" means a minor or intermittent impact to a non-operational element of the BT Cloud SIEM Service, for example a temporary failure of reporting or billing.

"**Priority 5 Technical Incident**" means an incident which has no direct impact on the BT Cloud SIEM Service. Records are used for information purposes. Example: to track upgrades, for planned outages or for enquiries as well as customer provoked Incidents.

"**Professional Services**" means those services provided by BT which are labour related services and are delivered remotely and charged at day rates unless otherwise set out in any applicable Order.

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

"**Reasonable Use Policy**" has the meaning given in Paragraph 2.7.2(b)(v).

"**Renewal Period**" means for each BT Cloud SIEM 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 of us.

"**RCA Support**" means assistance in identifying the root cause of a Security Incident or issue and may include support for customer RCA including by reporting on breaks or unwanted actions and recommending fixes or mitigating actions.

"**Schedule**" means the Managed Service Schedule to which this Annex is attached or can be found at www.bt.com/terms, and which forms part of the contract.

"**Security Case Assessment Notification Target**" means the time from classifying and advising you of a Security Incident to recommending a course of action to you.

"**Service Credit Interval**" has the meaning given in the table at Paragraph 10.2.1 for the relevant SLA Category.

"**Service Desk**" means the helpdesk that you will be able to contact to submit BT Cloud SIEM Service requests, report Technical Incidents and ask questions about the BT Cloud SIEM Service.

"**Security Event Classification Notification Target**" means the time from the BT SOC being made aware of an Event, classifying it and advising you of the classification of such Event.

"**Security Incident**" means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempt underway) exploitation of an existing vulnerability, and that has a significant probability of compromising business operations and threatening information security.

"**Security Incident Notification**" has the meaning given in Paragraph 10.4.1.

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

"**Service Level**" means the Availability Service Level set out in Part C.

"**Service Management Boundary**" has the meaning given in Paragraph 4.1.

"**Service Optimisation Manager**" or "**SOM**" means the security manager appointed by BT who will provide support to you in respect of certain activities as set out in this Annex.

"**Service Option**" has the meaning given in Paragraph 3.

"**Security Posture**" means the overarching approach to security adopted within your company.

"**Service Start Date**" has the meaning given in Paragraph 9.2.6.

"**Service Target**" means any target that BT aims to meet as set out in this Annex.

"**SIEM**" means security information and event management.

"**Silent Device Alarm**" means that an alarm is triggered when a device does not send any Logs for a set threshold, therefore warranting further investigation.

"**Simple Change**" means the Simple Changes set out in the document titled Simple and Complex Change which may be accessed on the Security Portal.

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

"**SLA Category**" means the category, as set out in any applicable Order, which, in accordance with the table set out at Paragraph 10.2.1, specifies the following in relation to the BT Cloud SIEM Service:

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

"**SOC**" means security operations centre.

"**SOM**" or "**BT SOM**" means the security operations manager BT appoints to liaise with you on Initial Setup and Controlled Deployment matters as set out in this Annex.
"**Standard Change**" means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements.
"**Standard Default Rule Set**" means a set of rules that BT can apply to your SIEM to allow for monitoring by BT, as set out in the Customer Service Description.
"**Standard Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 10.2.1 for the relevant SLA Category.
"**Strong Access Control**" means the use of security controls such as two-factor authentication to ensure that access to the BT Cloud SIEM Service is strongly secured.
"**Supplier**" if applicable, means the supplier of the Cloud SIEM Devices as set out in the applicable Order.
"**Supplier Annex**" if applicable, means the annex attached to the applicable Order, which sets out the Supplier details and related information for the various Cloud SIEM Devices on offer.
"**Supported Device List**" means the list of Event Log Data sources that are readily compatible with the Supplier's Cloud SIEM Devices as set out in the Supplier Annex (if applicable) attached to the applicable Order, and as may be amended by the Supplier from time-to-time.
"**Technical Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Cloud SIEM Service or particular element of the BT Cloud SIEM Service.
"**Urgent Change**" means in respect of a Simple Change 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.
"**Usage Volume**" means the agreed usage volume as set out in the applicable Order and calculated on your average EPS used in the calendar month.
"**User Guides**" means the documents that set out details on how you:

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

"**Vulnerability**" means a software susceptibility that may be exploited by an attacker.