G Cloud 15: SOC & SIEM

VODAFONE BUSINESS SECURITY ENHANCED

Contents

1. The Service – Overview

1.1 The Vodafone Business Security Enhanced ("VBSE") managed Security Operations Centre ("SOC") & Security Incident and Event Management system ("SIEM") (collectively known as the "Service" or "Services") is a set of services that are designed to use a combination of techniques to detect anomalous behaviour on Monitored Assets and proactively find, avoid or mitigate cyber-attacks and malicious activity before they cause material business impact to the Buyer. VBSE is a division of Vodafone dedicated to protecting critical national infrastructure, based in secure locations, and staffed by UK security cleared personnel. The Service is part of a portfolio of security services offered by VBSE.

1.2 The term "**Service**" or "**Services**" in these Service Specific Terms means the SOC & SIEM Service.

2. Service Term Structure

2.1 These Service Terms form part of the Call-Off Contract entered into under the G Cloud 15 Framework.

2.2 The Call-Off Contract comprises the Call-Off Order Form, the Supplier's Service Terms, Service Definition and Pricing Document, and the applicable Call-Off Terms and Conditions.

2.3 These Service Terms describe how the Service operates and apply in conjunction with the Call-Off Contract.

2.4 In the event of any conflict or inconsistency between these Service Terms and the Call-Off Contract, the Call-Off Contract shall prevail.

3. General Conditions on the Buyer

The Service is available to Buyers that meet and agree the following criteria:

3.1 Additional Service Recipient:

3.1.1. If Buyer wishes to add an Additional Service Recipient, then Buyer shall:

(a) provide the full corporate details of the Additional Service Recipient;

(b) seek approval in writing from Supplier;

(c) inform the Additional Service Recipient of the contractual arrangements; and

(d) agree to pay such additional Charges as Supplier may reasonably request in relation to the approval of such requests.

3.2 Authorised Users: Access by Buyer to the Services and Equipment is limited to authorised Users. Buyer is responsible for ensuring Users' compliance with this Agreement.

3.2.1. If Supplier provides each authorised User with User Details, Buyer is responsible for:

(a) the security of User Details; and

(b) providing Supplier with the identity of the authorised Users and keeping that information current.

3.2.2. Supplier accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions relating to the User Details up until the time that it informs Supplier that they are being used without authority or may be compromised.

3.3 AUP: Buyer shall comply with the AUP in using the Services.

3.4 Third Parties: Buyer shall ensure that the Users and all Additional Service Recipients (if any) comply with this Agreement in relation to their use of the Services and Equipment and shall be liable to Supplier for the acts and omissions of the Users and all Additional Service Recipients (if any) in relation to this Agreement. Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-licence the Services or Equipment (except Buyer Equipment) to any third party.

3.5 Terms of Use: Buyer shall not:

(a) make unauthorised modifications to the Services;

(b) use the Services as a means to establish permanent servers, relay connections or interconnection services or any similar commercial activities;

(c) do anything that causes the Network to be impaired;

(d) use automated means to make calls and/or texts or to send data (including via a GSM Gateway), unless expressly authorised in this Agreement;

(e) use the Services in a way that:

(i) may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in violation of any person's rights; or

(ii) is illegal, fraudulent or contrary to good faith or commercial practice to Supplier's detriment; or

(f) use the Supplier's SMS service to send mass notification messages, or mass marketing messages, whether or not the messages are unsolicited unless expressly authorised in this Agreement.

3.6 Service Monitoring: Buyer gives express consent for Supplier to monitor Buyer's use of the Service (and disclosing and otherwise using the information obtained) to the extent allowed by Applicable Law to:

(a) comply with Applicable Law;

(b) protect the Network from misuse;

(c) protect the integrity of the public internet and/or Supplier's systems and Networks;

(d) determine if Buyer has breached any conditions or restrictions on use of the Service;

(e) provide the Service; and/or

(f) take any other actions agreed or requested by Buyer.

3.7 Compatibility: Buyer shall ensure its systems, equipment and processes satisfy any Technical Prerequisites and if required to be used in conjunction with the Equipment and/or the Services, are in good working order (if applicable) and are compatible for use with the Equipment and/or the Services. Supplier shall use reasonable endeavours to advise Buyer of relevant requirements on request, but in no event shall Supplier be responsible for any performance or non-performance issues with the Equipment and/or the Services, or liable to support the Equipment and/or the Services, if Buyer's systems, equipment, or processes fail to satisfy the Technical Prerequisites or are otherwise incompatible with the Equipment and/or the Services. Supplier may suspend the provision of any Service for which Technical Prerequisites have not been procured within the specified period and charge Buyer any applicable Recovery Charge.

3.8 Security and Misuse: Buyer shall take reasonable steps in line with commercial good practice with entities it controls to limit misuse of or threat to the Service or Network; and address any misuse or threat identified by Supplier through the implementation of appropriate security or user controls. Buyer shall not run any security tests, vulnerability scans or penetration tests on Supplier Equipment or Services without Supplier's prior written approval.

3.9 Unauthorised Equipment or Repairs: Buyer acknowledges that:

(a) Equipment or Buyer Equipment not authorised for use on the Network; or

(b) any unauthorised attempt to repair or tamper with the Equipment,

may result in an impaired User experience and/or invalidate the manufacturer's warranty.

3.10 End of Life

3.10.1. **Notification:** Where Equipment is End of Life, Supplier may, on provision of reasonable notice:

(a) retire the Equipment; and/or

(b) provide the Buyer with an option of replacement Equipment which provides equivalent or improved functionality to the extent that alternatives are available.

3.10.2. **Replacement:** Where End of Life Equipment is replaced in accordance with clause 3.10.1(Notification), the costs of such replacement shall be charged to Buyer a One-Off Charge and invoiced accordingly.

3.10.3. **Continued Use:** Where, following receipt of an End of Life notification in accordance with this clause, Buyer continues to use End of Life Equipment, or does not use its best endeavours to allow Supplier to replace the End Of Life Equipment, Supplier:

(a) shall have no maintenance obligations for the End of Life Equipment;

(b) shall not be liable for Buyer's use of the End of Life Equipment;

(c) shall not be liable for any service levels relating to the Equipment; and

(d) reserves the right to suspend all or part of the affected service.

3.11 Buyer Equipment: Where Buyer provides Buyer Equipment for use with a Service, Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service):

(a) install and configure the Buyer Equipment at Buyer Sites by the date necessary to allow Supplier to perform its obligations;

(b) maintain the Buyer Equipment to Supplier's satisfaction, including prompt installation of security patches and updates;

(c) immediately replace any Buyer Equipment which is declared by its manufacturer as end-of-life (or otherwise stops marketing, selling or supporting it) and notify Supplier of any such replacement;

(d) promptly after the Service terminates, give Supplier access to and reasonable help with disconnecting Buyer Equipment from the Service; and

(e) warrant and undertake that Buyer has full authority to permit Supplier to perform the Service using the Buyer Equipment.

3.12 Exclusions:

3.12.1. Supplier does not guarantee that the Services will be continuously available and/or fault-free and Buyer acknowledges that faults may occur from time to time. This acknowledgement is without prejudice to any specific service levels agreed between the Parties in this Agreement.

3.12.2. Buyer is responsible for satisfying itself that the Services and any Equipment are suitable for its intended purpose and requirements (including but not limited to any resiliency and/or business continuity requirements). Supplier does not warrant or represent that the Services and Equipment are or will be fit for Buyer's intended purpose and requirements. Supplier recommends that Buyer obtains business continuity (or other) insurance that is appropriate for the nature of its business.

3.12.3. Supplier is not responsible for any content, goods or services which are accessed, downloaded or transmitted by Buyer through use of the Services. Supplier accepts no responsibility for any such content, goods or services. Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.

3.12.4. Buyer acknowledges that the Service is not intended for use by Consumers in the European Union. Without prejudice to the foregoing, the Buyer shall immediately notify Supplier if it becomes aware that anyone other than Supplier has made available, or intends to make available, the Service to a Consumer in the European Union.

3.13 Termination: Where Buyer terminates the Call-Off Contract during the Call-Off Contract Period, the Buyer agrees to pay Supplier's reasonable, committed and unavoidable losses resulting from the termination of the Call-Off Contract.

3.14 Network Sunset

3.14.1. Buyer hereby acknowledges and accepts that:

(a) certain Network technologies used to provide the Service on Supplier Equipment or Buyer Equipment may retire prior to the expiry of the contract; and/or

(b) current Networks may be replaced by further advanced Network technologies during the term of the Call-Off Contract.

3.14.2. As a result, Buyer agrees that maintaining compatibility of its devices with the available Networks from time to time shall be its responsibility.

3.15 Planned Service Changes by Third-Party Providers: Supplier has been informed that BT Openreach (the "Third-Party Provider") for legacy PSTN is withdrawing the service, with full switch off expected to be complete by 31 January 2027. Supplier is entitled to move the Buyer from legacy PSTN to Ethernet Access Method as and when required. Buyer will be advised of an alternative Service Element and the associated Charges, as set out in these Service Terms below. Buyer will have the option to either order an alternative Service Element or to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

3.16 Interpretation: In this Agreement, unless the context otherwise requires, words in the singular include the plural and vice versa.

3.17 Format: If Buyer requires this Agreement (or any bills, communications or a document referred to in this Agreement) in a different format, call 03333 043 222 or email disability.access@vodafone.co.uk for a large print, braille version, dyslexia-friendly or audio CD version. These contact details are for accessibility help only.

4. Fixed Services Conditions on the Buyer

4.1 Service Commencement Date: Buyer shall notify Supplier within 5 Working Days of the Service Commencement Date if, in the Buyer's reasonable opinion, the Services do not conform to the standard testing criteria and provide sufficient supporting details. Upon receipt of Buyer's notification, Supplier shall take reasonable action to meet the standard testing criteria.

4.2 Supplier-Owned Equipment: The following will apply where Supplier provides Fixed Equipment for Buyer's use with a Service:

4.2.1. **Title:** Title to the Fixed Equipment at all times belongs to Supplier, its suppliers or subcontractors (subject only to any rights which may be granted to Buyer in respect of Supplier Software, as set out in these Service Terms).

4.2.2. **Buyer Obligations:**

4.2.3.1 Buyer agrees to:

(a) provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;

(b) use the Fixed Equipment only for the purpose of using the Services, in accordance with Supplier's instructions and Applicable Law;

(c) allow only Supplier's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);

(d) adequately insure for, and notify Supplier immediately of loss, breach or suspected breach or damage to the Fixed Equipment;

(e) only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Supplier;

(f) provide Supplier with:

(i) adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites; and

(ii) in the case of BPE patch cords and cabling; and

(iii) 10 Supplier Working Days' notice of any known disruptive event (such as power disconnection).

4.2.3.2 Additionally, specifically in relation to BPE, Buyer shall:

(g) appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and

(h) ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular:

(i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and

(ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.

4.2.3. **Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service

4.2.4. install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Supplier to perform its obligations;

(a) Maintain the Buyer Equipment including prompt installation of security patches and updates;

(b) Promptly after the Service terminates, give Supplier access to, and reasonable help with, disconnecting Buyer Equipment from the Service; and

(c) Warrant and undertake that Buyer has full authority to permit Supplier to perform the Services using the Buyer Equipment.

4.3 Buyer Sites: For the purposes of preparing for and delivery of the Services, Buyer shall:

(a) carry out, or permit Supplier or its subcontractors to conduct, a Site Survey;

(b) prepare the Buyer Site for the Services in accordance with Supplier's instructions;

(c) allow and/or have in place (or assist Supplier to do so at Buyer's cost) all third-party consents necessary to allow Supplier or its subcontractors and agents (and obtain consents from third parties to allow) to:

(i) access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third-party property located there, as Supplier reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and

(ii) ensure that Buyer Sites are safe and have a suitable working environment.

4.4 Emergency Services:

4.4.1. **General**: In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, and/or a failure of the internet connection on which the Service relies, Buyer may not be able to make calls including calls to emergency services. This may also affect any calls using the internet including calls to emergency services.

4.4.2. **Buyer Obligations**: Buyer shall:

(a) provide Supplier with complete and accurate Buyer Site address information; and

(b) give Supplier at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information.

4.4.2.1 Buyer acknowledges that any failure to provide the information required in 4.4.2 may render emergency services unable to identify User's location.

4.5 Calls Using the Internet: Where a Service places calls using the internet, Buyer shall:

4.5.1. Make Users accessing the Service via a soft client aware that Supplier may be unable to automatically determine their location if they make an emergency services call using the Services.

4.5.2. Ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service.

4.5.3. Provide a registered address where a Buyer or User will make calls over the internet including if there are multiple addresses where such calls will be made and keep information on all such locations up to date.

4.6 **Survey:** These Service Terms and each Service Element are subject to survey. In the event a Site Survey output results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and the Call-Off Contract.

4.7 **Third-Party Costs:** Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Supplier by third parties in connection with the provision of the Services. Such Charges (often referred to as Excess Construction Charges) are detailed in the Professional Services section of these Service Terms. These Charges will be notified to the Buyer before any construction works take place. In the event this results an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

5. Service Specific Conditions of Use

5.1 **Buyer obligations:** The Buyer shall use the Service only in accordance with the terms and obligations as indicated in the Agreement and includes:

(a) **Third Party Providers:** Service Elements may be provided by a subcontractor of Supplier. Additional terms and conditions may apply to those Service Elements;

(b) **Adequate Buyer Personnel:** Buyer must provide adequate personnel as may be reasonably requested by Supplier to assist Supplier to implement and perform the Services. Such Buyer appointed personnel may include: (i) a representative who has authority to make financial and contractual decisions relating to the Agreement (the "Buyer Representative"), (ii) a point of contact with relevant technical expertise and knowledge of the Buyer's business and environment to act as an escalation route for the duration of the project design and implementation of the Service (the "Project Lead"), and (iii) at least one central administrative/security contact to handle Security Incident reports from the SOC and available on a 24x7x365 basis (the "Authorised Security Contact"). The Buyer must keep the list of the Buyer appointed personnel up to date and shall notify Supplier immediately of any changes;

(c) **Project Plan:** Buyer must carry out the tasks allocated to the Buyer under any Project Plan agreed with the Buyer Project Lead;

(d) **Access to Buyer Software / Hardware:** Buyer must provide Supplier (and any third party engaged by Supplier in connection with the Services) access to software and hardware that is covered by, or required for, the Services at reasonable times in accordance with Buyer's standard security procedures;

(e) **Access to Monitored Assets:** Buyer shall be responsible for providing Supplier with access at all times to the Buyer's environment (including, but not limited to, Monitored Assets, Buyer Sites, and Buyer's network) to enable Supplier to provide support and/or carry out replacements or repairs in the event of any system failure;

(f) **Site Access:** Buyer must provide the relevant contact details and Buyer Site access procedures and grant timely site access to Supplier as appropriate to install, maintain and decommission the Service;

(g) **Configuration:** Buyer is responsible for installing and maintaining their log servers, Monitored Assets and equipment as well as any equipment or Software Agents supplied by Supplier. The Buyer is responsible for ensuring that the necessary communication protocols can traverse Buyer networks, and for making any necessary changes to enable delivery of the Service including ensuring its firewalls are configured for onward connectivity to Supplier's data centre(s);

(h) **Compliance with Terms:** Buyer must comply with any other obligations ascribed to the Buyer as set out in these Service Specific Terms, or elsewhere in the Agreement or as reasonably notified to Buyer by Supplier from time to time;

(i) **Provision of Technical Data and Other Information:** Buyer must provide to Supplier all technical data and other information Supplier may reasonably request to enable Supplier to supply the Service;

(j) **Contextual Information:** Buyer must identify, keep up to date and provide full and accurate information about the Monitored Assets from across the Buyer environment to enable the SOC to assess Security Events and inform the Buyer whether it requires further investigation ('Contextual Information'). Below is a non-exhaustive indicative list of the types of Contextual Information the Buyer must provide to Supplier in a timely manner:

(i) Network architecture diagrams;

(ii) Expected data flows;

(iii) Server and network asset data (IP addresses, patch levels, backup profiles etc);

(iv) Relevant business processes that affect traffic flows and patterns;

(v) Specific activities/events that will change the normal traffic patterns;

(vi) Normal working hours;

(vii) Changes to software releases, patches or new application code introduction;

Where Supplier is operating the underlying service, much of this Contextual Information will be collated and managed by Supplier. It is the Buyer's responsibility to ensure that any relevant Contextual Information under the Buyer's control is passed to Supplier in a timely fashion;

(k) **Compliance with Technical Prerequisites:** Buyer must ensure that the Buyer's systems comply with all Technical Prerequisites for supply of the Services reasonably notified to the Buyer in advance by Supplier;

(l) **Security Scans:** Buyer shall notify Supplier in writing, and obtain the agreement in writing of Supplier, prior to carrying out any security scans;

(m) **Power:** Buyer must provide and ensure the continued maintenance of a suitable power supply for all equipment associated with the Service that is deployed to a Buyer Site. Buyer shall contact Supplier for details of the power requirements of Service equipment. Where a Resilient Solution is provided, Supplier recommends that the Buyer uses independent power supplies for each path in the Service;

(n) **Connectivity:**

(i) (i) The Services require appropriate connectivity in place to enable Supplier's remote management. Supplier recommends a minimum of 10Mbps per connection. The Buyer acknowledges that loss of connectivity may result in loss of Security Event Logs and temporary loss of Service and Supplier shall not be liable for failing to meet the Service Levels or to pay Service Credits in this regard;

(ii) (ii) If user and entity behaviour analytics is required as part of the Service then the Buyer shall provide connections to their active directory ("AD") via lightweight directory access protocol ("**LDAP**").

(o) **Time Accuracy:** Buyer must ensure all Monitored Assets are synchronised with an accurate and common time source (e.g. Network Time Protocol) to enable correlation of Security Event Logs. Buyer must ensure that accurate and common time is present in all Security Event Logs presented to the Service. Logs for all Monitored Assets must be provided to Supplier in a suitable timestamped format;

(p) **Environment for Supplier Equipment:** Buyer shall ensure the provision and continued maintenance of an appropriate environment for all equipment associated with the Service deployed to a Buyer Site including suitable power and cooling complying with operating conditions as specified by the relevant hardware manufacturer or Supplier;

(q) **Notification of Buyer Changes:** Without prejudice to the other provisions of this Agreement, Buyer must inform Supplier at least 1 working day in advance of any operational or business changes that may impact the Service (e.g. maintenance, upgrades, false positives, penetration testing, power outages and disconnections) ("Buyer Change"). If the planned change is expected to be temporary, the Buyer will provide the following information:

(i) Anticipated start date / time of change window;

(ii) Anticipated end date / time of change window;

(iii) Nature of the Buyer Change and likely impact on the Service; and

(iv) Details of the Authorised Security Contact.

The Buyer will inform Supplier when Buyer Change has ended or if the change window has been extended;

(r) **Security Event or Security Incident Reporting:** Buyer must immediately report any Security Events or Security Incidents that breach or threaten to breach the security of the Service to the SOC. The Buyer must report to the SOC in a timely manner any known threat or activity that is actively or currently targeting the Buyer;

(s) **Buyer Third Parties:** Buyer must engage and manage its third parties as required to support delivery of the Service;

(t) **Third Party Software:** Supplier may use certain third party supplied products ("Third-Party Software") in its provision of the Service. The Buyer agrees and acknowledges that Buyer will not have access to these products. Any output directly from the Third-Party Software that is used by Supplier in connection with the Service to the Buyer without further input from Supplier will be provided on an "as is" basis and is excluded from any warranties which may be set out in this Agreement. Supplier may change the Third-Party Software it uses during the provision of the Services, provided that such changes do not have a material adverse impact to the Service.

(u) **No Re-selling:** Buyer shall not re-sell, sub-lease, sub-rent or sub-license part or all of the Services;

(v) **Further Buyer Obligations:** Buyer shall comply with the requirements set out in this Agreement and provide all reasonable assistance as may be required by Supplier to perform the Services;

5.2 Limitations:

5.2.1. **Excluded Events:** Supplier shall have no responsibility or liability for any breach of the Agreement, or for failure or delay in performing its obligations, and shall have no obligation to pay Service Credits, where the breach, delay, or failure to meet a Service Level occurs as a result of or in connection with an Excluded Event.

5.2.2. **Attacks on Monitored Assets:** Buyer acknowledges and agrees that:

(i) It is not possible for the Service to detect all potential attacks on Monitored Assets;

(ii) The Service is only part of a defence in depth approach to securing assets, of which the Service is just one security control; and

(iii) Supplier excludes any liability for any damage resultant from all and any attempted or successful attacks on Monitored Assets.

5.3 General Assumptions and Dependencies

5.3.1. The Service is not warranted to help Buyer comply with any Applicable Law, industry standard or Buyer's internal policies other than those set out in the Agreement.

5.3.2. It is Buyer's sole responsibility to determine and provide adequate security for the Buyer's environment and Monitored Assets.

5.3.3. Buyer must promptly notify Supplier of any changes to information, provided by Buyer to Supplier, in relation to the Service.

5.3.4. Supplier may provide reasonable recommendations, advice or instructions on a particular course of action in the course of performing, or as a result of, the Service to be provided to Buyer. If Buyer chooses not to follow such reasonable recommendations, advice or instructions, Buyer acknowledges that Supplier shall not be responsible for any losses incurred, or claims made, by the Buyer that arise from Buyer's failure to follow such recommendations, advice or instructions.

5.4 Changes

5.4.1. Buyer is responsible for all Buyer's costs and updating of Buyer systems as a result of any changes made under this clause 5.

5.4.2. Supplier may make changes to the Service in accordance with the Framework Agreement.

5.5 Operational Changes

5.5.1. A change constitutes an "Operational Change" if:

(a) it is a technical or operational change which does not impact the Service or the agreed timescales for the provision of the Service; and

(b) it applies to Services that are already delivered and in service.

5.5.2. Operational Changes include changes such as modifications to firewall rule-bases, changes to tuneable operating system parameters, and installation of patches.

5.5.3. Operational Changes may be requested and implemented by way of the "Operational Change Management Procedure", which is set out in clause 6.3 below.

5.5.4. The Operational Change Management Procedure is not intended to be used:

(a) to resolve any loss of Service performance; or

(b) to deliver new Services.

5.5.5. Supplier will categorise Operational Changes into the following categories at Supplier's absolute discretion:

(a) **Emergency Change:** an Operational Change:

(i) which is required to prevent the occurrence of a severity 1 or severity 2 Service Incident specified in clause 3.1 of Annex 2 Service Levels;

(ii) where the failure to implement the requested Operational Change would have a material and detrimental impact on Supplier's ability to provide the Services to the Buyer; and/or

(iii) where the circumstances of the Operational Change necessitate Supplier providing an expedited response.

(b) **Routine Change:** an unplanned Operational Change which is not an emergency change.

Supplier will respond to Emergency Changes in priority to Routine Changes. Buyer must respond to Emergency Changes raised by Supplier promptly.

5.6 Operational Change Management Procedure

5.6.1. The procedure for reviewing, processing and recording requested Operational Changes is as follows

(a) in the case of an Emergency Change:

(i) Emergency Changes must be raised with Supplier or by Supplier with the Buyer via telephone and electronically;

(ii) Buyer must only declare genuine Emergency Changes and Supplier reserves the right to downgrade an Emergency Change if, in Supplier's reasonable opinion, it is not a genuine emergency or Buyer makes excessive use of this facility; and

(iii) Supplier will record and review the request for the Emergency Change and contact the Buyer with a committed action in respect of the Emergency Change.

(b) In the case of a Routine Change:

(i) Routine Changes must be raised with Supplier electronically; and

(ii) Supplier will record and review the request for the Routine Change and contact the Buyer with a committed action in respect of the Routine Change.

5.7 Planned Works

5.7.1. Supplier will use reasonable endeavours to provide the Buyer with at least 10 Working Days' notice of any Planned Works affecting the Buyer.

5.7.2. Buyer may not refuse Planned Works that Supplier requires to ensure the integrity, supportability, security, performance or availability of any infrastructure for the Buyer or Supplier's other customers.

5.7.3. Supplier will use reasonable endeavours to ensure that the Planned Works are not carried out in a way that affects the Services provided to Buyer in a materially detrimental way.

5.8 Additions and Removals of Monitored Assets

5.8.1. **Inclusive Additions:** The Charges include the addition of up to a total number of Monitored Assets set out in the Order Form per calendar month, subject to:

(a) the type of device(s);

(b) the device(s) having an existing log parser configuration and log path into the SIEM; and

(c) the total number of Monitored Assets and EPS not exceeding the total number of Monitored Assets and combined EPS set out in the Order Form

("Inclusive Additions").

5.8.2. The Buyer shall follow the Operating Change procedure set out in clause 5.5 for any Inclusive Additions. Supplier shall endeavour to perform the additions within five (5) Working Days of the request.

(a) **Inclusive Removals:** The Charges include the removal of up to the total number of Monitored Assets set out in the Order Form per calendar month as a single activity ("Inclusive Removals"). The Buyer shall follow the Operational Change procedure set out in clause 5.5 to request any Inclusive Removals.

(b) **Removals:** Removals beyond the Inclusive Removals shall be subject review by Supplier to determine the Professional Service Charges based on the agreed rate card. The number of days required to perform the removals will be confirmed and agreed in writing between the Parties before the activity begins by way of a contract amendment or new Order Form (as determined by Supplier).

(c) **Additions:** The Buyer may request additional Monitored Assets to be included to the Service ("Additions"). If the number of Monitored Assets is greater than the Inclusive Additions, the Buyer may request additional Professional Services of one (1) day for up to five (5) additional Monitored Asset based on the agreed rate card. This clause 5.8(d) shall apply depending on the type of device(s) and providing:

(i) the device(s) have an existing log parser configuration and log path into the SIEM;

(ii) the EPS of the total number of Monitored Assets do not exceed those agreed by the Parties in the Order Form.

Any Additions shall be agreed in writing between the Parties by way of a contractual amendment or new Order Form (as determined by Supplier), in accordance with the General Terms.

(d) Additional Charges shall apply to the following activities:

(i) where a new log parser configuration or log path into the SIEM is required;

(ii) addition of servers for new applications, incorporating devices for new departments;

(iii) onboarding new Monitored Assets to the Service; and

(iv) additional EPS to those set out in the Order Form.

In respect of the activities listed in this clause, Supplier will assess the requirements with the Buyer and determine the applicable Charges. The activities and applicable Charges will be agreed in writing between the Parties before the activities begin by way of a contract amendment or a new Order Form (as determined by Supplier).

(e) **Total EPS reviews**: Supplier will evaluate the net EPS of the Monitored Assets on a quarterly basis against the agreed EPS. In the event that the total number of EPS exceeds the agreed EPS, the Buyer shall pay the additional Charges associated with the excess EPS or Supplier shall have the right to reduce the level of the Service at no liability to the Buyer. The calculation and rate of the additional Charges will be specified in the Commercial Terms or Order Form.

6. Data Protection

Supplier as a Data Controller

6.1 **Supplier as a Data Controller:** Supplier acts as an independent Data Controller for the Processing activities in these clauses 6.1 to 6.5 (Data Controller role and processing activities) and any additional activities listed in the Service Terms.

6.2 **Buyer as a Data Controller:** The Parties acknowledge that Buyer will also act as an independent Data Controller for any Personal Data relating to Supplier employees or representatives, for example business contact information.

6.3 **Processing Activities:** Supplier may process:

6.3.1. Personal Data to:

(a) manage account relationships;

(b) send bills;

(c) fulfil an Order or delivery;

(d) provide customer service; and

(e) control access to Supplier's systems that support the Services.

6.3.2. As an electronic communications service's provider, Traffic Data in accordance with Applicable Laws to:

(a) deliver User communications;

(b) calculate Charges for each User;

(c) identify threats to the Network or Services and protect against them; and

(d) internally develop and improve the Network or Services.

6.4 **Data Disclosures:** Supplier may disclose Personal Data and Traffic Data:

(a) to Vodafone Group or third parties for the purpose of supporting the Processing activities described in this clause 6 (Data Protection) or as permitted under Applicable Privacy Law; and

(b) as required by Applicable Law, court order, or any Authority (including Privacy).

6.5 **Privacy Notice:** Supplier's privacy notice can be accessed at: www.vodafone.co.uk/privacy.

Supplier as a Data Processor

6.6 **Supplier as a Data Processor:** Supplier acts as a Data Processor for the specific processing as set out in the relevant Service Terms.

6.7 **Processing Personal Data:** Supplier may only Process Personal Data on behalf of the Buyer:

(a) to provide and monitor a Service as outlined in the Service Terms; or

(b) for any other purpose agreed in writing between the Parties. Additional instructions from Buyer require prior written agreement and may be subject to Charges.

6.8 **Changes to Sub-Processors:** If Supplier adds or replaces a Sub-Processor, Supplier shall inform the Buyer of changes to Sub-Processors where Supplier is required by Applicable Privacy Law by:

(a) providing at least 10 Working Days' prior notice; or

(b) listing the new or replacement Sub-Processor on www.vodafone.co.uk at least 10 Working Days before Supplier authorises and permits the new or replacement Sub-Processor access to Personal Data in order to give the Buyer the opportunity to reasonably object to such changes.

6.9 **Sub-Processor Obligations:** Supplier will enter into binding agreements with its Sub-Processors, who will have substantially the same legal obligations for Processing activities as Supplier under these clauses 6.6 to 66.17 (Data Processor role and related requirements). Supplier will be liable to Buyer for the performance of that Sub-Processor's obligations.

6.10 **Data Retention:** Supplier may keep Personal Data for as long as required to deliver the Service. After this Agreement is terminated, and unless Applicable Law requires otherwise, Supplier will:

(a) delete the data within a reasonable time frame;

(b) return the data if the Buyer provides notification before termination of the Agreement.

6.11 **Data Access:** Supplier may give access to Personal Data only if necessary to meet its obligations in relation to the Service and will take reasonable steps to ensure that whoever accesses the data:

(a) is under a statutory or contractual obligation of confidentiality;

(b) is trained in Supplier's policies for handling Personal Data; and

(c) does not Process Personal Data except as instructed by Buyer, unless Applicable Law requires otherwise.

6.12 **Data Security:**

6.12.1. As required by Applicable Privacy Law, Supplier will:

(a) provide technical and organisational measures for a level of security appropriate to the risk presented by Processing taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing;

(b) comply with Supplier information security policies based on ISO / IEC 27001:2013;

(c) give Buyer all information, assistance, and co-operation it may reasonably require to comply with Applicable Privacy Law;

(d) notify Buyer without undue delay of any unauthorised access to Personal Data that results in loss or unauthorised disclosure of, or alteration to, Personal Data;

(e) provide reasonable assistance to Buyer in relation to any Personal Data breach notification that Buyer is required to make under Applicable Privacy Law; and

(f) when requested by Buyer and before any Processing, provide reasonable assistance with:

(i) carrying out a privacy impact assessment of the Services; and

(ii) consulting the relevant Privacy Authority regarding Processing activities related to the Services.

6.12.2. Further information on data security measures can be found at www.vodafone.com/business/customer-security.

6.13 **Audits and Inspections:** If Buyer has a right of audit and inspection under Applicable Privacy Law, it agrees to act as follows:

(a) Buyer may ask to review Supplier's security organisation, and the good practice and industry standards contained in Supplier's information security policies no more than once each calendar year, and any such review shall relate only to data protection compliance of the Services; and

(b) ensure its instructions comply with Applicable Privacy Law. Supplier will inform Buyer if it believes any Buyer instruction infringes Applicable Privacy Law or any confidentiality obligations.

6.14 **Buyer Responsibilities:** Buyer accepts and agrees that they are responsible for:

(a) reviewing the information Supplier makes available; and

(b) determining if the Services meet Buyer's requirements and legal obligations.

6.15 **Onward Transfers out of the EEA and UK:** Supplier may onward transfer Personal Data to a country outside the European Economic Area, the UK or a country that has not been designated by the European Commission or Secretary of State in the UK as ensuring an adequate level of protection under Applicable Privacy Law, only if:

(a) the data is transferred in line with the requirements under Applicable Privacy Law;

(b) the Processing or transfer does not put any Buyer in breach of Applicable Privacy Law; or

(c) Applicable Law requires it. In this case, Supplier will inform Buyer of that legal requirement before Processing, unless prohibited by Applicable Law.

6.16 **Law Enforcement:** Supplier:

(a) may receive legally binding demands from a law enforcement authority for the disclosure of, or assistance with Personal Data, or be required by Applicable Law to disclose Personal Data to persons other than Buyer ("Demand");

(b) is not in breach of any obligation to Buyer in complying with the Demand; and

(c) will notify Buyer of the Demand as soon as possible, unless prohibited by Applicable Law.

6.17 **Data Subject Enquiries:** Taking into consideration the nature of the data processing conducted by Supplier on behalf of the Buyer, Supplier shall assist the Buyer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Buyer's obligation to respond to requests for exercising the data subjects' rights laid down in Applicable Privacy Law.

7. Service Elements

7.1 Supplier will monitor the Monitored Assets agreed with the Buyer by assessing ingested Security Events through a Security Event Log aggregator and comparing against agreed Use-Cases for detection of anomalous and potentially malicious behaviour. Supplier uses threat intelligence feeds from different sources to identify security threats; these sources include national cyber authorities, commercial and open sources as well as its own developed threat intelligence sources. The Service includes near real time analysis and alerts through the SIEM platform.

7.2 Security Events flagged by the SIEM system are analysed by Supplier's cyber security analysts within the SOC. If a Security Event is deemed a Security Incident (as set out in the Playbook), Supplier will report to the Buyer in accordance with the terms of this Agreement. Supplier will investigate the Security Incident and provide an explanation to the Buyer and recommend how the Security Incident should be addressed in accordance with the terms of this Agreement.

7.3 The Service shall comprise the following Service Elements:

7.3.1. Core Service Elements which shall include:

(a) **Secure Log Collection and SIEM Platforms**: Security Event Log collection from the Monitored Assets and SIEM services will be supplied by Supplier;

(b) **Security Event Collection**: Supplier will collect Security Events from Monitored Assets and retain them for further analysis;

(c) **Security Event Monitoring and Analysis**: Supplier will provide the Buyer with:

(i) access to its SOC on a 24x7x365 basis, an integrated Security Incident Management function; and

(ii) monthly management reports in such format as Supplier may reasonably determine;

(d) **Management: Central management by Supplier including maintenance, configuration and fault management and fixing;**

(e) **Proactive Monitoring: Standard proactive monitoring;**

(f) **Connectivity: Supplier may provide VPN connectivity configuration as part of the Service; and**

(g) **Service Levels**: for Service Availability and Service Incident resolution (further details of which are provided in Annex 2).

7.3.2. Optional Service Elements, where selected, which shall include:

(a) **Secure Communications Network**: the method of connectivity to enable the Monitored Assets to connect to the Service and enable the Security Event Logs to be collected;

(b) **Resilience Options**: Resilient and Non-Resilient Solutions are available for deployment in Supplier data centres and at the Buyer Site(s); and/or

(c) **Professional Services**: may include a Project Manager, Service Level Management or other technical or specialist advisor.

7.3.3. Each Service Element may have a different Service Commencement Date and Minimum Term as detailed in these Service Specific Terms or specified in the Call-Off Order Form and/or this Agreement.

7.3.4. Before commencement of the Services, Supplier will design, build and implement the Services as set out below:

(a) **Project Manager:** Supplier may assign a Project Manager to oversee the design and implementation of the Services in an effective and timely manner, depending on the complexity of the Buyer's requirements and the project. In the event that Supplier assigns a Project Manager, the Project Manager will be responsible for:

(i) agreeing with the Buyer any specific requirements and required delivery timescales;

(ii) co-ordinating the delivery of required hardware, software and service integration; and

(iii) acting as the single liaison point for all Buyer contact until the Service is fully operational.

(b) **Project Plan**: Before the Service Commencement Date, Supplier will provide the Buyer with a document giving an overview of the Solution as agreed in consultation with Buyer. The Buyer shall meet with Supplier as necessary to agree a plan which shall include the implementation timelines, scope, management and administrative measures necessary to roll out and commence performance of the Services (the "**Project Plan").**

(c) **Design:** Supplier will engage with the Buyer to review the Solution and the Project Plan and commence development of the Playbook. Buyer acknowledges and agrees that this will entail capturing the Buyer's Managed Assets IP addresses, hostnames, any threat history, and/or any Buyer threat intelligence as well as the review of any applicable Buyer security policy to identify how the Security Events will be reported and escalated by the Service.

(d) **Build:** Supplier will procure any equipment, hardware and software licences that may be required for the performance of the Services, and the Buyer shall pay for any such equipment, hardware and software licences, set out in the Order Form (as further amended in accordance with this Agreement). Supplier will install and configure dedicated virtual servers to act as aggregation points for capture of Security Event Log feeds from across the Monitored Assets and configure its firewalls for onward feed to the SIEM. Upon completion of the build phase, Supplier will test connectivity to start gathering Security Event Logs. Supplier will perform a standard set of tests of the configurations to ensure the configurations set out in the Playbook have been mapped correctly and that the Security Events Logs are flowing from the Monitored Assets to the SIEM. At the point that all tests have been performed successfully, the Solution will be considered live and proceed to Service Baselining.

(e) **Service Baselining:** Buyer acknowledges and agrees that:

(i) After the build phase, the Service requires a period of Service Baselining which may take in the region of three months depending on the complexity of the Buyer's requirements and the Buyer's environment;

(ii) During the Service Baselining period, the Service will be operational albeit some Security Events and/or Service Incidents may not be responded to as quickly and accurately as set out in the Playbook;

(iii) During the Service Baselining period, Supplier and the Buyer will update and finalise the Playbook and Supplier may carry out further configurations of the systems in line with the Playbook; and

(iv) Supplier will inform the Buyer when the Service Baselining has ended, and the Service is fully operational.

(f) Buyer acknowledges and agrees that:

(i) The set up and implementation period of the Service will be estimated and specified in the Order Form; and

(ii) Any lead time quoted by Supplier is subject to change and will commence on completion of the approved design.

7.4 Installation of the Service at Buyer Site:

7.4.1. Supplier's engineers or engineers of Supplier's sub-contractors (collectively referred to as "Engineers") shall be responsible, on Supplier's behalf, for installation and maintenance of the hardware delivered and managed as part of the Services.

7.4.2. Where the hardware is installed on a Buyer Site, Supplier will ensure the hardware is fitted, racked, powered and connected to the Buyer's LAN, all of which the Buyer must ensure is provided and ready in advance of any Engineers attending the relevant Buyer Site(s). Supplier reserves the right to charge the Buyer for costs incurred in respect of the Engineers attending any Buyer Site at which the agreed Buyer Prerequisites (as set out in these Service Specific Terms and/or the Order Form) are not provisioned. Once the Engineers have ascertained evidence of connectivity, the Engineers will then remotely configure and manage the device.

7.5 Supplier will notify the Buyer when the Services are fully operational after which the following provisions shall apply:

(a) Supplier will perform the monitoring Services in accordance with the Playbook. If the underlying Security Event source changes over time (e.g. a new version of software or configuration on a Monitored Asset) or the Buyer requires further tuning or suppression of Security Events then the Buyer may request the optional Professional Services to re-configure the Service and to update the Playbook at an additional cost and shall follow the Operational Change procedure set out in clause 6.2 of these Service Specific Terms. Supplier will not be liable where changes to the underlying Monitored Asset mean that the specific element of the Service cannot continue to function as intended.

(b) Supplier will monitor the operating system events of the Monitored Assets only and the monitoring shall not include any additional applications unless otherwise specified in the Order Form.

(c) Supplier's offer is based on the number of Managed Assets and combined EPS set out in the Order Form. Monitored Assets or EPS may be added to the Service by way of a contractual amendment or new Order Form which will, for the avoidance of doubt, be subject to additional charges.

(d) Buyer acknowledges and agrees that the Service provides the resource levels required to monitor a reasonably managed and secured environment. Should the Buyer's environment require sustained, disproportionate resource, Supplier and the Buyer (acting in good faith) will review usage and endeavour to agree the changes by way of a contractual amendment. If the Parties cannot agree a contractual amendment, Supplier may suspend the Services and the Parties shall follow the Escalation Procedure set out in clause 6 of Annex 1. A 'sustained, disproportionate resource' may include but is not limited to, a single Monitored Asset or multiple Monitored Assets generating, on more than one isolated occasion, a higher number of Security Events and/or Security Incidents than Supplier would expect (in Supplier's absolute discretion) a Monitored Asset(s) of that nature to generate. Supplier reserves the right to charge the Buyer for any additional resource Supplier is compelled to assign to the Buyer to provide the Services in addition to those envisaged in the Agreement.

(e) No security service can guarantee 100% protection and therefore, Supplier can accept no liability for any damage or loss resulting directly or indirectly from any failure of the Services to detect anomalous behaviour.

8. Service Level Agreement

8.1 The Service Levels are set out in Annex 2 of these Service Terms.

9. General Definitions

9.1 The following definitions apply to the **section 3 - General Conditions on the Buyer** of these Service Terms:

Additional Service Recipient	a Buyer Group entity which is not a direct party to this Agreement, but which is named in this Agreement as a beneficiary of the Services or otherwise approved to receive the Services in accordance with clause 3.1 (Additional Service Recipient).
Agreement	this agreement, consisting of the documents set out in clause 2 (Service Terms Structure).
Applicable Law	law, regulation, binding code of practice, rule or requirement of any relevant government or governmental agency, regulatory Authority, each as relevant to (i) Supplier in the provision of the Services and/or (ii) Buyer in the receipt of the Services or the carrying out of its business.
AUP	Supplier's acceptable use policy set out at http://www.vodafone.co.uk/Acceptable-Use-Policy-Business, as updated by Supplier from time to time.
Buyer	the entity identified in the Call-Off Order Form as such.
Buyer Equipment	hardware, software or any other tangible material not supplied by Supplier that is used with or to access the Service. Any Equipment Buyer purchases from Supplier shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Group	Buyer and any company in which Buyer has the beneficial ownership of more than 50% of the issued share capital, or the legal power to direct the general management of the company in question, either at or after the date of this Agreement.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Supplier needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Order Form.
Charges	the charges or fees specified in this Agreement as payable by Buyer.
Consumer	means any natural person acting for purposes that are outside the person's trade, business, craft or profession.
End Of Life	where Supplier or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Equipment	hardware, Supplier Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Supplier to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
European Union (EU)	an economic and political union of 27 countries, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea.
GSM Gateway	any equipment containing a SIM which enables calls from a fixed network (landline) to be routed via a GSM link to a mobile network establishing a mobile-to-mobile ('on-net') call.
Incumbent Provider	a regulated operator who is authorised to provide a Service in a given country.
Intellectual Property Rights	(a) rights in, and in relation to, any patents, registered designs, design rights, trade marks, trade and business names (including all goodwill associated with any trade marks or trade and business names), copyright, moral rights, databases, domain names, topography rights and utility models, and includes the benefit of all registrations of,

	applications to register and the right to apply for registration of any of the foregoing items and all rights in the nature of any of the foregoing items, each for their full term (including any extensions or renewals) and wherever in the world enforceable; (b) rights in the nature of unfair competition rights and rights to sue for passing off; and (c) trade secrets, confidentiality know how, technical information and other proprietary rights.
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Supplier to perform the Services.
Non-Recurring Charges	means One-Off Charges.
One-Off Charges	the Non-Recurring Charges payable by Buyer in relation to the Service and/or Equipment as described in the Commercial Terms and/or in Buyer's Call-Off Order Form, and may include installation Charges for ports, access circuits and routers, charges for set up of Service Elements and configuration changes.
Party or Parties	Buyer and/or Supplier, as relevant.
Recovery Charge	any amount payable by Buyer for early termination or failure to meet commercial commitments as set out in this Agreement.
Service Element	the individual components of a Service (including optional service elements if applicable).
Service Specific Terms	the document(s) identified in this Agreement as the "Service Specific Terms" that set out information such as terms and conditions, specifications and technical information specific to a Service.
Service(s)	the services to be provided by Supplier or a Third Party Provider under this Agreement and as specified in this Agreement. Any reference to Service within this Agreement may be an individual Service or collectively all Services, as appropriate.
SIM	a "subscriber identity module" card is an integrated circuit, whether physical or embedded in a device (and then known as an eSIM Card), storing user specific data and provided by Supplier to allow use of equipment on the Network by Buyer.
Supplier	where used in these Service Terms or the Call-Off Contract means Vodafone.
Supplier Software	any Software supplied by Supplier or its licensors to Buyer (including Software embedded in any Equipment).
Technical Prerequisites	any requirements detailed in the Service Specific Terms or otherwise provided to Buyer in writing relating to a Service or Equipment including notification to upgrade.
Third Party Provider	a third party contracted directly or indirectly by either Supplier (including Vodafone Group) or Buyer that provides a Service, a Third Party Service or that provides a service that connects to a Service. Third Party Providers may include Incumbent Providers.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer or an Additional Service Recipient unless otherwise specified in this Agreement.
User Details	a user name, password, or other access information used by a User to access the Service and/or Equipment.
UK	England, Wales, Scotland, Northern Ireland and adjacent islands (e.g. Isle of Wight) but excluding the Channel Islands and the Isle of Man.

Vodafone	Vodafone Limited, registered number 01471587, and registered office Vodafone House, The Connection, Newbury, Berkshire RG14 2FN.
Vodafone Group	(a) Vodafone Group Plc, Vodafone Limited and any company in which Vodafone Group Plc owns (directly or indirectly) 15% or more of the issued share capital; and (b) any partner market listed on the "Where we are" page at http://www.vodafone.com/.
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	9.00am to 5.00pm on a Working Day.

9.2 The following definitions apply to the Fixed Services Conditions on the Buyer set out in section 4 of these Service Terms:

BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
Fixed Equipment	hardware, Supplier Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Supplier to Buyer for use in receiving the Services.
Service Commencement Date	the date of completion of Supplier's testing when the Service is ready for use.
Site Survey	a survey of a Buyer's Site to assess whether (in Supplier's opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.

9.3 The following definitions apply to the Service Specific Conditions on the Buyer and Service Elements set out in section 5 of these Service Terms:

Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Supplier needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Order
Emergency Change	Means an Operational Change set out in clause 6.2 of the Service Specific Terms.
EPS	Events Per Second is the way the SIEM capacity is measured and is dependent on the type and number of Monitored Assets as specified in the Order Form.
Excluded Event	Any of the following: (a) any fault in, or any other problem associated with Buyer-supplied; electricity or other Buyer-supplied power source, hardware, software, non-maintained structured cabling or other telecommunications network or systems not provided by Supplier; (b) any fault, or negligent act or omission on the part of: (i) any third party that is not within Supplier's direct control; or (ii) the Buyer (c) any suspension of the Services in accordance with the provisions of the Agreement, or otherwise agreed between the Parties; (d) any other circumstances caused by events for which Supplier has expressly excluded liability in accordance with the provisions of this Agreement (including these Service Specific Terms);

	(e) any delay or failure of the Buyer to fulfil or perform its obligations under the Agreement (including, but not limited to, the obligations set out in clause 0 of these Service Specific Terms; (f) a fault or incident with another Supplier service purchased under a separate agreement; (g) a Service Incident, delay, or breach of this Agreement resulting from a request by Buyer for expedited delivery of the Service; (h) Buyer's request to modify or test a Service Element; (i) a Force Majeure Event; (j) a Service Request during implementation of the Solution; (k) a Service Incident caused by service failure at any other Buyer Site; (l) Planned Works; (m) Any breach of the Agreement by the Buyer, failure, or delay to performance in relation to equipment and/or Supplier Software which has been modified or changed on the Buyer's behalf and where Supplier has not agreed that such modification or change will not affect Supplier's liability to pay Service Credits; (n) a breach of the Agreement, failure or delay in performance, or Service Incident which arises as a result of the Buyer failing to agree to the installation of an upgrade, patch or change recommended by Supplier; and/or (o) any circumstances where Engineers cannot for any reason gain access to a location with on-site hardware required for provision of the Service.
EDS/IPS	Intrusion Detection System / Intrusion Prevention System. These technologies typically use pattern-matching (signatures) to detect potential events of interest.
Incident, Problem and Change Management	An ITIL approach that prioritises the core goals of problem, change and incident management to effectively manage the Service.
Monitored Asset	The equipment, device or application to which the Service is provided, as set out in the Order Form, subject to any subsequent amendments or changes which are agreed between the Parties and documented in writing.

Non-Resilient Service	Buyer's connection to one Supplier data centre.
Order Form	The document prepared by Supplier that specifies the Charges for the Services, as well as the specific elements and quantities of the Service required by the Buyer.
Planned Works	Planned Supplier-initiated changes to the Service or equipment (including, for example, activities undertaken to carry out routine or essential maintenance or upgrades, or to take preventative actions to support the running of Supplier's infrastructure).
Playbook	A document created by Supplier in conjunction with the Buyer during the design and implementation phase of the Services which specifies the Use-Cases and how the Buyer wishes Supplier to respond to certain security alerts, alert prioritisation, classification of Security Events and Security Incidents types and thresholds. Supplier will use the Playbook in the performance of the Services.
Professional Services	The optional services provided by Supplier in order to customise the Solution, perform additional services based on the Buyer's individual requirements, project manage the Solution, Service Level Management, make changes to the configuration of the Service and/or update the Playbook.
Quarterly Measurement Period	The period from the Service Level Commencement Date up to the end of the calendar quarter and then each calendar quarter thereafter (save for the last quarter that will end upon the termination date of the Service).
Resilient Service	Buyer's connection to two or more Supplier data centres.
Routine Change	Means a Routine Change set out in clause 5.5 (e) (ii) of the Service Specific Terms.
Security Event	An incidence of anomalous behaviour on a Monitored Asset.
Security Event Log	A log of Security Events.
Security Incident	A Security Event which in the reasonable opinion of Supplier requires further investigation and analysis.
Security Incident Management	The end-to-end management of Security Incidents by Supplier.
Security Incident Response	Supplier's response to a Security Incident, as set out in clauses 2.2 Annex1 and clause 5 of Annex 2.
Services	the services (which consist of Fixed Services and/or Mobility Services, and which include any applicable Service Elements) to be provided by Supplier or a Third Party Provider

	under this Agreement and as specified in this Agreement. Any reference to Service within this Agreement may be an individual Service or collectively all Services, as appropriate
Service Availability Service Level	The percentage of time the Service or Service Element (as applicable) is available for use in a Quarterly Measurement Period.
Service Baselining	The fine tuning and mapping of Security Event Log collection, event rules and triggers for the Monitored Assets.
Service Credits	The service credit payable by Supplier to the Buyer in accordance with these Service Specific Terms, in particular Annex 2 (Service Levels).
Service Incident	An unplanned interruption to the Service, a reduction in the quality of a Service, or a failure of a Service configuration item.
Service Level(s)	The service levels that apply to the provision of the Service as set out in Annex 2 to these Service Specific Terms.
Service Level Commencement Date	In respect of the Service, or an individual Service Element (if applicable) the later of: (i) the end of the Service Baselining period; or (ii) the Service Commencement Date, for such Service or individual Service Element (as applicable).
Service Request	A minor Buyer request for a standard or catalogue pre-approved change that is low risk, relatively common and follows a standard procedure (for example, a password reset), and excluding Operational Changes.
Service Support	The support services provided by Supplier under the agreement as set out in clause 1 of Annex 2.
Software Agent	Any software provided to the Buyer by Supplier to enable delivery of Security Event Logs to the Service.
Solution	A combination of Service Elements tailored to address the Buyer's specific needs and requirements, defined in the Order Form, as may be subsequently supplemented or amended in accordance with these Service Specific Terms.
Trouble Ticket	A record of a Service Incident with a unique reference allocated to it that is used for all subsequent updates and communications.
Use-Case	A change in activities, use or the architecture in the Monitored Assets or a Buyer requirement that may give rise to Security Event or Security Incident, as further described in the Playbook.

Working Hours	Monday-Friday 0900-1700, excluding public holidays in the United Kingdom.

9.4 The following definitions apply to **section 6 - Data Protection** of these Service Terms:

Applicable Privacy Law	the relevant data protection and privacy law, regulations (including UK GDPR and the Data Protection Act 2018) and other regulatory requirements to which Vodafone Limited is subject.
"Fixed Authority	means those governments, agencies, courts of law, and professional and regulatory authorities including NRAs that supervise, regulate, investigate, or enforce Applicable Law.
Data Controller	the person that determines the purposes and means for which Personal Data is Processed, as defined under Applicable Privacy Law.
Data Privacy Obligations	in respect of each Party, that Party's obligations relating to the Processing or control of Personal Data as a Data Controller or Data Processor, as expressly set out in clause **Error! Reference source not found.** (Data Protection) of this Agreement.
Data Processor	the person that Processes Personal Data on behalf of the Data Controller as defined under Applicable Privacy Law.
European Economic Area (EEA)	means the Member States of the European Union together with Iceland, Liechtenstein, and Norway, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea.
GDPR	General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data.
Personal Data	shall mean any information relating to an identified or identifiable natural person as defined by the Applicable Privacy Law.
Privacy Authority	the relevant statutory or supervisory authority with responsibility for the Applicable Privacy Law in the jurisdiction of the Data Controller.
Process/Processed/ Processing/ Processes	obtaining, recording or holding information or data or carrying out any operation or set of operations on it.
Sub-Processor	a sub-contractor who is processing Personal Data on behalf of Supplier.
Traffic Data	any data processed for the purpose of the conveyance of a communication on an electronic communications network and for billing.
UK GDPR	means GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

ANNEX 1

SERVICE SPECIFICATION

1. Service Design and Implementation

1.1 **The Delivery Phases:** The Services will be performed in phases. Buyer acknowledges and agrees that each phase must be fully completed before the next phase will begin. Buyer must complete the Prerequisites defined by Supplier before phases three and four will begin. Supplier is not responsible for any performance or non-performance issues with the Service caused by Buyer Prerequisites or Buyer failing to comply with the Buyer Prerequisites. During each phase, Supplier will assess the results of the interviews and/or workshops and either continue with the Service as set out in the Order Form, or review the possibility of modifying the Order Form by way of a contract amendment. The phases are set out below:

(a) **Phase One – Project Initiation and Planning:** During this phase, Supplier shall assist Buyer with defining and compiling requirements and develops a Project Plan.

(b) **Phase Two – System Design:** Supplier shall undertake architectural and system design for Buyer's environment. If the SIEM System is already deployed, Supplier shall perform a design review.

(c) **Phase Three – Implementation**: If not already deployed, Supplier shall install and configure the SIEM System components and verifies that data is being transmitted and reported.

(d) **Phase Four – Integration and Transition**: Supplier shall develop processes and corresponding documentation and shall begin transitioning management and monitoring to the SOC.

(e) **Phase Five – Ongoing Operational Support**: During this phase, Supplier shall provide steady state management and monitoring of the SIEM infrastructure.

2. Features

2.1 **SOC Analysis and Alerting**

(a) The Service includes 24x7x365 support from the SOC. The SOC utilises SIEM technology that processes all the Security Event Logs generated by the Service and a skilled security analyst resource within the SOC to investigate the generated alerts.

(b) The key components of this Service Element are:

(i) acceptance of Security Events from the Monitored Assets;

(ii) generation of Security Incident tickets on Supplier ticket systems if Security Event Log collection issues are detected;

(iii) correlation of Security Events and near real time alerts that meet the triggers defined in the Playbook;

(iv) trend analysis of Security Event data to detect suspicious activity;

(v) initial investigation of alerts prior to escalation or closure;

(vi) escalation of all Security Incidents to the Authorised Security Contact; and

(vii) maintenance of records of Security Events and Security Incident Response activity (from creation to closure) for all alerts raised (regardless of whether they are true or false positive alerts);

2.2 **Security Incident Response**

(a) The SOC will act as a first responder in relation to any Security Incidents raised. The SOC has no access to any of the Monitored Assets (unless agreed otherwise). Buyer acknowledges and agrees that Security Incident Response is therefore a joint function between the SOC and Buyer. The key Security Incident Response steps are:

(i) Security Incident assessment and escalation to the Buyer as appropriate;

(ii) Security Incident prioritisation and categorisation;

(iii) Isolation and preservation - preserve any Security Event Logs (as requested by the Buyer);

(iv) Security Incident Recovery – coordinate with the Buyer to restore the Service to operation;

(v) Engaging forensic services – provide reasonable assistance to the Buyer appointed forensics team; and

(vi) Security Event tuning - implement any changes to the Service recommended by the SOC or the Buyer as a result of a Security Incident investigation using the Operational Change process set out in clauses 6.2 and 6.3 of the Service Specific Terms.

2.3 **Reporting**

(a) The Order Form will confirm the level of reporting included in the Service.

(b) The Service can include reporting to provide historical and trending information across the month in review to the Buyer (as determined by Supplier), and will typically comprise:

(i) A high-level data summary;

(ii) Graphical and/or tabular evidence;

(iii) Firewall traffic profiles (if applicable);

(iv) Summarisation of any IDS/IPS signatures triggered;

(v) Details of Security Incidents raised throughout the reporting period; and

(vi) Any actions for the Buyer to undertake.

2.4 **Security Event Log File Retention and Access**

(a) Security Event Log data collected and processed by the Service will be retained for the period specified in the Order Form.

(b) Subject to the provisions of this clause 2.4, in the event of a Security Incident (whether detected by the Service or not) that the Buyer deems serious enough to warrant further investigation (by the Buyer or their appointed forensic investigators or law enforcement), the Buyer may request access to the Security Event data held by Supplier to facilitate the investigation. Supplier will provide reasonable assistance where requested to support any such investigation.

(c) Supplier will make Security Event Log data available to the Buyer upon written request (provided the data is within the contracted retention period). The method of making this data available to the Buyer will be agreed between the Parties at the time of request.

(d) The Service does not provide for Buyer access to the SIEM or to any data generated by the SIEM platform.

(e) Buyer acknowledges and agrees that:

(i) The Security Event Logs are parsed and enriched with additional data by the Service before they are stored in the SIEM. As a result, these logs are not appropriate for use during forensic analysis as part of post-incident activities; and

(ii) The Buyer should not rely on the Service for forensic logging of their Monitored Assets.

3. Facility & Network Services

3.1 The SIEM and SOC are located at VBSE operational centres. Each of these VBSE centres apply an integrated approach to physical security in which a range of protective security measures deliver a "defence in depth" capability. These measures include:

(a) Manned Guarding – this includes 24/7 support for each site and each security officer is Security Industry Authority (SIA) registered;

(b) External and internal CCTV;

(c) Perimeter intruder detection;

(d) Access control systems;

(e) NPSA (National Protective Security Authority) rated rooms, cabinets and locks;

(f) Internal intruder alarms;

(g) Fire detection and suppression systems; and

(h) Redundant power, cooling and network architectures with generator backup.

4. Service Support

4.1 The Service Support model is an IT Infrastructure Library (**"ITIL"**) aligned support structure integrating standard support agencies and key ITIL functions such as Incident, Problem and Change Management.

4.2 The Service is a fully monitored, managed and maintained service, supported 24x7x365.

4.3 **Service Levels:** Supplier shall provide the Service in accordance with the Service Levels and Service Credits set out in Annex 2.

5. Service Level Management

5.1 Supplier provides a Professional Service option for Service Level Management ("SLM") deliverables. If applicable, the Order Form will specify the SLM deliverables included in the Service.

5.2 SLM is a fundamental part of Supplier's Service Support model providing specialised additional services alongside Supplier's standard business support functions.

5.3 Supplier SLM aims to (i) meet and exceed agreed service delivery and performance targets, and (ii) ensure future services are also delivered in the same way.

5.4 **Service Level Management (SLM) Key features**

(a) The table below sets out the SLM key features that are standard to the Service(s) unless otherwise stated in the Order Form:

Deliverables	Detail / Frequency
Service Manager resource	Supplier office based
Buyer Satisfaction Surveys; regular surveys to collate Buyer feedback. Linked to service improvement and development plans.	Bi-annual
Monthly Service Reports; detailing performance against service level targets and proactively identifying performance trends requiring improvement or development	Monthly
Service Level performance analysis; Improvement actions tracked with clear deadlines for progress and resolution.	10 days post reporting period
Service Reviews; monthly joint business review to drive service quality and efficiency in line with Buyer goals and priorities.	By phone (monthly)
Service Improvement Plans; Improvement actions tracked with clear deadlines for progress and resolution.	Yes
Knowledge Management; Buyer specific document production, storage and inventory management.	Bi-annual
Contact Model - Specialist to Specialist, e.g. security specialists, technical analysts etc.	Yes

6. **Escalation Procedures**

6.1 Supplier has established an operational and hierarchical escalation processes which may be used by the Buyer to address operational or non-operational issues or any other matters that are not resolved within the SLA.

6.2 **Operational Escalations**

(a) These can be initiated at any point in the lifecycle of an incident, change or new provisioning activity if the Buyer feels that the Service Level target is in danger of not being met or the support mechanisms in place to manage and resolve an issue are not working.

(b) Operational escalations should in all cases be made by telephone, whereas hierarchical escalations can be made by telephone or email.

(c) **Operational Escalations Table (incidents & changes):**

Level	Title	Criteria	% of Target Time to Restore (depending on Severity Level) elapsed since the beginning of the Incident
1	SOC Analyst	SLA at risk of not being met No action plan or path to resolution within SLA Lack of response or co-operation	75%
2	SOC Manager & Service Manager (if assigned)	SLA at risk of not being met No action plan or path to resolution within SLA Previous action plan failed Lack of response or co-operation	90%
3	Sector Service Lead &/or Head of Sales	SLA missed No action plan or path to resolution within SLA Previous action plan failed Lack of response or co-operation	100%
4	Head of VBSE	No action plan or path to resolution Missed 2 x SLA or agreed action plan failed Lack of response or co-operation breach	Breach

(d) **Operational Escalations Table (new orders/provisioning):**

Level	Title	Criteria	% of Target Time to Restore (depending on Severity Level) elapsed since the beginning of the Incident
1	Project Manager or Implementation Manager	Agreed Delivery Date at risk of not being met No action plan or path to resolution Lack of response or co-operation	50%
2	Programme Manager	Agreed Delivery Date at risk of not being met No action plan or path to resolution Previous action plan failed Lack of response or co-operation	75%
3	Sector Service Lead &/or Head of Sales	Agreed Delivery Date at risk of not being met No action plan or path to resolution Previous action plan failed Lack of response or co-operation	90%
4	Head of VBSE	No action plan or path to resolution	Breach

		Agreed Delivery Date and action plan failed Lack of response or co-operation	

6.3 **Hierarchical Escalations:** These can take place at any time to resolve issues that relate to a dispute with the Agreement, persistent breach of Service Levels, service performance calculations or if the Buyer is unsatisfied with how operational escalations are being handled.

Level	Account/Contract related	Support/Performance related	Timescale
1	Account Manager	Service Manager (if assigned)	To be agreed with the Buyer at each level and dependant on the nature of the escalation
2	Account Sector lead	Sector Service lead	To be agreed with the Buyer at each level and dependant on the nature of the escalation
3	Head of VBSE		
4	Senior Manager Vodafone Business		

ANNEX 2:

SERVICE LEVELS

1. General Support Services Terms

1.1 Supplier will provide the Buyer with a Support Service for the Service Elements specified in the Order Form.

1.2 The Support Service is available in English only.

1.3 The Support Service is available as shown below:

Support Service	Service Cover Period
Service Incident Management for Severity Level 1 & 2 Service Incidents	24/7
Service Incident Management for Severity Level 3 & 4 Service Incidents	Working Hours
Service Request Fulfilment	Working Hours

1.4 Service Incidents may be reported at any time during the Service Cover Period set out in the table above, however, Service Incident resolution will only occur during Working Hours for severity level 3 and 4 Service Incidents.

1.5 The Buyer must appoint primary and secondary central points of contact responsible for accessing the Support Service and communicating with Supplier during the relevant Service Cover Period. The Buyer will inform Supplier, and keep Supplier up-to-date with the appointed individuals' identity and level of access.

1.6 The Buyer will:

(a) reimburse Supplier for reasonable expenses associated with actions taken when the Buyer has reported a Service Incident caused by an Excluded Event; and

(b) permit Supplier to interrupt the Service to resolve a severity level 1 or 2 Service Incident (and if no permission is granted then the relevant Service Incident will be downgraded to a severity level 3 Service Incident).

1.7 Supplier may temporarily interrupt the Service to carry out Planned Works. Supplier will endeavour to notify the Buyer in advance of any Planned Works. Any interruption in the Services connected with the Planned Works shall affect the Service Levels.

1.8 **Service Incident Commencement and Resolution Rules:**

(a) A Service Incident:

(i) commences when Supplier creates a Service Incident report (being no later than 60 minutes after the Service Incident has been reported to Supplier); and

(ii) ends on the earlier of when Supplier advises the Buyer of a Service Incident resolution or when the Service Incident affecting the Service has ceased.

(b) At Supplier's discretion or at the Buyer's reasonable request, Supplier may continue to investigate using Supplier's internal problem management procedures, however, this shall not affect the resolved status of the Service Incident. The Buyer is deemed to have been advised of Service Incident resolution if Supplier has made reasonable attempts to contact the Buyer and the Buyer has not notified Supplier within 24 hours from Supplier's last attempt to contact the Buyer that the Service Incident resolution is unsuccessful. Supplier's method of Service Incident resolution is at Supplier's sole discretion.

2. **Calculation**

(a) "Service Availability" is expressed as a percentage ("P"), and calculated as: P= ((A-B)/A) x 100, where:

(i) "A" equals the number of minutes in the Quarterly Measurement Period; and

(ii) "B" equals the number of whole minutes when the relevant Service or Service Element is unavailable in the Quarterly Measurement Period.

2. Availability Service Level

(a) The Service Level for Service Availability of the Solution ("Availability Service Level") is specified in the Order Form, and will detail at least the following:

(i) the Service Availability offered; and

(ii) any exclusions.

(b) The Availability Service Level excludes scheduled outages for maintenance, configuration changes that require re-boot(s) and changes that have been approved in accordance with clause 6 (Changes) of the Service Specific Terms. Service Availability calculations exclude any interruption to the Service due to faults in, or any other problem associated with, Buyer-supplied WAN, electricity, hardware, software, non-maintained structured cabling or other network or systems not provided by Supplier.

(c) Additionally, the maximum Availability Service Level that may be offered as specified in the Order Form is as per the table below. If there is any conflict between the Order Form and the table below, the lowest figure of the two relating to maximum Availability Service Level takes precedence.

Class of Service	Maximum Availability Service Level	Example
Non-resilient Solution	99.7%	Service provided with one or more single points of failure within the Supplier environment, such as a single log aggregation server or single firewall.
Resilient Solution	99.99%	Service provided from two VBSE locations with multiple, geographically diverse, log aggregation servers and firewalls.

3.Severity of Incidents

3.1 The following severity level classifications apply to the Service:

Severity Level	Severity Level Definitions
1 – Critical	A total loss of the Service. E.g. The Supplier SOC is unable to process or receive Security Event Logs.
2 – Significant	Partial loss of the Service which has a significant detrimental effect on Supplier's ability to perform normal operations but which does not represent a total loss of the Service. E.g. SIEM persistently fails to connect to Security Event Log aggregator server or does not receive Security Events from Security Event Log aggregator server within the expected period.
3 – Minor	Degradation of Service, such as loss of resilience, including a severity Level 1 or 2 Service Incident where Supplier has been denied access to a Buyer Site or Managed Asset or where Supplier has been unable to agree a period of maintenance activity (for reasons outside Supplier's reasonable control) to restore normal service.
4 – No service impact	Any Service Incident not classified as severity level 1, 2 or 3.

4. **Restoration Times Service Level**

4.1 The target time to resolve a Service Incident (the "Target Time to Restore") is dependent on the severity level of the Service Incident as set out in clause 3.1 of Annex 2 to these Service Specific Terms.

4.2 The elapsed time from the point at which Supplier raises a Trouble Ticket for the Service Incident to the point at which Supplier declares that, in Supplier's reasonable opinion, the Service or relevant Service Element has been restored, shall be known as the "Actual Time to Restore".

4.3 The Target Time to Restore for each severity level is as follows:

Severity Level	Target Time to Restore
1	4 Hours
2	8 Hours
3	24 Hours
4	72 Hours

5. **Security Incident Response**

5.1 A Security Incident is raised following initial investigation by the SOC. Security Incidents are not Service Incidents. Should there be an actual Service Incident, a separate Service Incident ticket will be raised.

5.2 The SOC operates to the following targets:

(a) Security Incidents will be notified to the Buyer within 60 minutes of detection by the SOC;

(b) investigation reports will be provided to the Buyer within 24 hours of notification of Security Incident conclusion; and

(c) reports will be provided to the Buyer within an agreed week of the month following the final date to which the report relates.

6. Service Credits

6.1 **General Service Credit Terms:** Buyer acknowledges and agrees that:

(a) Service Levels and Service Credit terms for the Service or applicable Service Element commence on the Service Level Commencement Date.

(b) Service Credits are calculated as follows:

(i) Service Credits for Service Incident Resolution Target are calculated and reported monthly;

(ii) Service Credits for Availability Service Level are calculated and reported quarterly; and

(iii) Service Credits are expressed as a percentage of the Monthly Recurring Charge ("MRC") for the Service.

(c) Service Credits do not apply for any failure or delay in performing the Service that arises out of, or in connection with, an Excluded Event.

(d) Where the failure to meet a Service Level impacts another Supplier service, the Buyer shall be entitled only to Service Credits relating to the affected Service Element under this Agreement.

(e) If one Service Incident causes a failure of two or more Service Levels, only the greater Service Credit amount of the two (or more) Service Levels shall be payable.

(f) Service Credits, as set out in this Annex 2, shall be the Buyer's sole and exclusive remedy against Supplier in respect of any failure in Service performance. Service Credits have been calculated as, and are, a genuine pre-estimate of the loss likely to be suffered by the Buyer for failure in Service performance. Service Credits may only be applied to Charges for the Service and have no cash value.

(g) Any Service Credits will be applied to the Buyer's next bill after such Service Credits become due. All Service Credits will only be payable if:

(i) Supplier proactively notified the Buyer that a Service Credit is payable; or

(ii) the Buyer notifies the Supplier representative that the Buyer believes a Service Credit is payable. Such notification is to be made in writing within 30 calendar days of the date of the relevant service failure which the Buyer believes gives rise to a Service Credit. Supplier will then investigate the claim for a Service Credit and confirm whether the Service Credit is payable.

(h) The following financial limits apply to Service Credits:

(i) in no event will Service Credits due for any accounting period exceed the associated recurring charge payable by the Buyer for that period; and

(ii) aggregate Service Credits (whether for breach of the Availability Service Level and/or the Restoration Times Service Level) in a measurement period will be capped at 40% of the aggregate MRC for the Solution.

6.2 **Service Credits for Failure to Meet the Availability Service Level**

Where the Service Availability in a Quarterly Measurement Period falls below the Availability Service Level, the Buyer shall be entitled to a Service Credit. The Service Credit available is dependent on the value of 'X' in the table below, where X is a positive number expressed as a percentage figure and calculated as (X = percentage Availability Service Level minus percentage Actual Service Availability).

X (= % Availability Service Level minus % Service Availability)	Service Credit (% of MRC)	
	Non-Resilient Solution	Resilient Solution
X is between 0.01% and 0.99% inclusive	None	2.5%
X is between 1.00% and 1.99% inclusive	2.5%	5.0%
X is between 2.00% and 2.99% inclusive	5.0%	10.0%
X is equal to or greater than 3.0%	10%	20.0%

6.3 **Service Credits for Failure to Meet the Service Incident Resolution Target:** Buyer acknowledges and agrees that:

(a) The "Service Incident Resolution Target" is the percentage of Service Incidents, in each calendar month following the Service Commencement Date, which are resolved within the Target Time to Restore (i.e. where the Actual Time to Restore is equivalent to or less than the Target Time to Restore).

(b) The Buyer is entitled to the following Service Credits where the Service Incident Resolution Target for Service Incidents of the relevant severity level is not achieved within a given calendar month.

(c) The Buyer is entitled to Service Credits for failure to meet Service Incident Resolution Targets only in relation to resolution of Service Incidents relating to the Monitored Assets and used in accordance with the terms of the Agreement.

(d) The time taken by the Buyer to resolve any Service Incident raised by Supplier will be excluded from the calculation of the Actual Time to Restore for the purposes of the Service Credit.

(e) Achievement of, or failure to achieve, the Service Incident Resolution Targets, is measured, reported and calculated each calendar month.

Severity level	Service Incident Resolution Target	Service Credit for failure to meet the Service Incident Resolution Target (% of monthly recurring charge)
1	100% of Service Incidents resolved within the Target Time to Restore	2.5.%
2	< 95% of Service Incidents resolved within the Target Time to Restore	2.5%
3	< 95% of Service Incidents resolved within the Target Time to Restore	2.5%
4	N/A	N/A