Appendix 6

Key Performance Indicators

These Key Performance Indicators are intended as templates for each customer, they may be amended as applicable to each subsequent contract, subject to the customer's requirements.

I. The KPIs which the Parties have agreed shall be used to measure the performance of the Services by the Supplier are contained in the below table.

II. The Supplier is required to manage and provide the Services in such a way as to meet the KPIs.

III. The Supplier shall monitor its performance against each Target KPI and shall send the Authority a monthly report detailing the achieved KPIs in a form and format to be mutually agreed.

An overview of the Service Level Agreement, including service hours & applicable response and fix times:

SLA	DESCRIPTION	SERVICE COVERAGE HOURS	SLA RESPONSE TIME	SERVICE LEVEL	EVENT GRADING
Security Information and event management	Business impacted or imminent impact expected within 4 hours; for example, sever cyber incident or SIEM platform full outage Customer cannot perform business critical functions; loss of revenue; risk of severe reputational damage; all end users unable to perform business critical roles. Highly likely to require Security Incident Response. A Security Incident created from the SOC analysing a security alert and identifying that it is a potential threat or breach that requires action from the customer. When the SOC determines that a security alert is a suspected security incident, it will be reported to customer within fifteen (15) minutes of identification.	24/7	<15 minutes	98%	GREEN >98% AMBER<97% RED<96% BLACK<95%
Security Information and event management	Moderate to high impact cyber incident or partial SIEM platform outage Risk to revenue generation; multiple end users unable to perform	24/7	<30 minutes	98%	GREEN >98% AMBER<97% RED<96% BLACK<95%

	business critical roles. May require Security Incident Response. A Security Incident created from the SOC analysing a security alert and identifying that it is a potential threat or breach that requires action from the customer. When the SOC determines that a security alert is a suspected security incident, it will be reported to customer within thirty (30) minutes of identification.				
Security Information and event management	Low to moderate impact cyber incident. Unlikely to require Security Incident response. A Security Incident created from the SOC analysing a security alert and identifying that it is a potential threat or breach that requires action from the customer. When the SOC determines that a security alert is a suspected security incident, it will be reported to customer within 4 hours of identification.	24/7	<4 hours	98%	GREEN >98% AMBER<97% RED<96% BLACK<95%
Security Information and event management	Very low impact cyber incident When the SOC determines that a security alert is a suspected security incident, it will be reported to customer within 1 week of identification.	24/7	1 week	98%	GREEN >98% AMBER<97% RED<96% BLACK<95%

Service Availability	SIEM service availability		Monthly availability level	99%	GREEN >99% AMBER <98% RED <97% BLACK <96%
Service Desk	Service Request – Working Hours only	M-F 0.900-18.00(ex-bank holidays)	<4 hours	98%	n/a
Change request	Standard change Pre-approved procedural change with minimum risk and impact to service	M-F 09.00-18.00 (ex-bank holidays)	<4 hours	95%	n/a
Change request	Normal change A change, which requires authorisation, is complex and/or requires down time for a related service.	M-F 09.00-18.00 (ex-bank holidays)	<4 hours	95%	n/a

For the avoidance of doubt the Supplier provides a Time To Action SLA and therefore the analysts will start working on events received within the Supplier platform within the specified period. Depending on the criticality of the event Softcat will notify the Authority inline with the communication methods and times stated in this contract.
For further avoidance of doubt, the supplier shall begin to review the log data once received onto the Supplier platform, within 2 hours.

Where the customer notifies the Supplier of an incident, this must be done by phone.

1. **Monitoring Performance**

1. Performance by the Supplier against each KPI shall be graded as follows:

Green Event	Meets the KPI
Amber Event	Some failure to meet the KPI which requires closer monitoring and plans for corrective action.
Red Event	Material failure to meet the KPI
Black Event	Significant failure to meet the KPI

2. The Supplier shall provide the Authority with a monthly performance report detailing its performance in respect of each of the Service Levels.
3. The Contract Managers shall have regular meetings to monitor and review the performance of this agreement, the achievement of the KPIs and the provision of the Services. Such meetings shall be minuted by the Supplier's Contract Manager and copies of those minutes shall be circulated to and approved by both parties.
4. Prior to each meeting, the Contract Managers shall notify each other of any problems relating to the provision of the Services for discussion at the meeting. At the meeting, the parties shall agree a plan to address such problems. Progress in implementing the plan shall be included in the agenda for the next meeting.
5. The Authority and the Supplier shall review the KPIs every three (3) months throughout the Contract Period and make any changes in accordance with the Change Control Process to reflect changes in the requirements for the Services.

2. **Service Level Failure**

1. A Service Level Failure shall occur where, in any one-month period:

Red Event	Registered against two KPIs

Black Event	Registered against one KPI

Service Credits

2. If there is a Service Level Failure, the Supplier shall:
   1. notify the Authority immediately of the Service Level Failure.
   2. otherwise, then in the occurrence of a Relief Event, automatically credit the Authority with the applicable service credits as described below ("**Service Credits**");
   3. provide the Authority with a draft remediation plan which sets out the steps to be taken by the Supplier in order to remedy the Service Level Failure and prevent recurrence ("**Remediation Plan**");
   4. deploy all additional resources and take all remedial action that is necessary to rectify or to prevent the Service Level Failure from recurring; and
   5. carry out the actions identified in Remediation Plan in accordance with its terms.

3. Other than in the following circumstances:
   1. Any negligent act or omission of the Authority.
   2. Any breach of an express provision of this Contract by the Authority.
   3. Any Force Majeure Event.

If there is a Service Level Failure, the Authority shall be entitled to a Service Credit equal to 2.5% of the monthly service period charges (based on the Fixed, Semi Fixed and Variable Costs), payable for affected service element(s) in that Month period.

4. Service Credits will be in the form of the Supplier issuing a credit note against a previous invoice and the amount for the Service Credits shall be repayable by the Supplier as a debt within thirty (30) Business Days of issue of the credit note. The parties agree that any such Service Credits have been calculated as, and are, a genuine pre-estimate of the loss likely to be suffered by the Authority.

The aggregate Service Credits for any month shall be capped at [three (3) Service Credits or 6% of the Contract Price payable for that month]

Relief Event means

(i) any breach of any express provision of this Contract by the Authority including without limitation an obligation to comply with the Authority's obligations.

(ii) any negligent act or omission of the Authority.

ii.any Force Majeure Event.