UK OFFICIAL

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	DDaT22536
THE BUYER:	UK Shared Business Services LTD (UK SBS)
BUYER ADDRESS	Polaris House, North Star Avenue, Swindon, SN2 1FL
THE SUPPLIER:	Insight Direct (UK) Limited
SUPPLIER ADDRESS:	4th floor The Charter Building, Charter Place, Uxbridge, UB8 1JG
REGISTRATION NUMBER:	02579852

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 5th May 2023.

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

- Lot 3 Software & Associated Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are

UK OFFICIAL

- Call-Off Schedules for **DDaT22536**
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 8 (Business Continuity & Disaster Recovery) Part B
  - Call-Off Schedule 11 (Installation Works)
  - Call-Off Schedule 20 (Call-Off Specification)

4 CCS Core Terms (version 3.0.6)

5 Joint Schedule 5 (Corporate Social Responsibility) RM6068

6 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

CALL-OFF START DATE:	Thursday 25th May 2023
CALL-OFF EXPIRY DATE:	Friday 31st July 2026
CALL-OFF INITIAL PERIOD:	36 months

CALL-OFF DELIVERABLES

2.2.3 Deliverables

1. All core software components installed and configured per the upgrade guide and best practice.
2. Deployment configuration signoff.

LOCATION FOR DELIVERY

Services are to be delivered remotely.

DATES FOR DELIVERY OF THE DELIVERABLES

Milestone/Deliverable	Description	Timeframe or Delivery Date
Installation	To run parallel with existing system to confirm usability and functionality	30/06/2023
Test	Dual running of installation to ensure we are seeing the same results	30/06/2023
Transfer	Transfer of service must be complete.	31/08/2023

TESTING OF DELIVERABLES

Option A: None

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 90 days from delivery against all obvious defects.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

Each party total aggregate liability in each Contract Year under each call-off contract (whether in tort, contract or otherwise) is no more than greater of £5 million or 150% of the Estimated yearly charges unless specified in the Call-Off order form

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £176,160.88.

CALL-OFF CHARGES

The total Call-Off contract value for the SIEM Solution Cloud Migration work and year 1,2 & 3 operational costs shall not exceed £455,980.88 Excluding VAT

MANDATORY CHARGES	
YEAR ONE	
[redacted]	
Total	**£176,160.88**

UK OFFICIAL

YEAR TWO	
[redacted]	
Total	**£139,910.00**
YEAR THREE	
[redacted]	
Total	**£139,910.00**
TOTAL CONTRACT VALUE	
Total	**£455,980.88**

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Payment to be made upfront on annual basis following successful submission of valid invoice. The contracting authority shall pay the supplier within 30 days of receipt of valid invoice.

Invoice must include valid and undisputed purchase order number.

BUYER'S INVOICE ADDRESS:

UK Shared Business Services

Polaris House, North Star Avenue, Swindon, SN2 1FL

finance@uksbs.co.uk

BUYER'S AUTHORISED REPRESENTATIVE

[redacted]

UK OFFICIAL

Polaris House, North Star Avenue, Swindon, SN2 1FL

[redacted]

BUYER'S ENVIRONMENTAL POLICY

N/A

BUYER'S SECURITY POLICY

N/A

SUPPLIER'S AUTHORISED REPRESENTATIVE

[redacted]

SUPPLIER'S CONTRACT MANAGER

[redacted]

KEY SUBCONTRACTOR(S)

Advanced Network Security Limited, Central 40, Chineham Business Park, Basingstoke, Hampshire, RG24 8GU

UK OFFICIAL

COMMERCIALLY SENSITIVE INFORMATION

Please see Joint Schedule 4

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

UK OFFICIAL

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** ("**CCS" "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: 7 **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

UK OFFICIAL

Joint Schedule 3 (Insurance Requirements)

The insurance you need to have

The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

the Call-Off Contract Effective Date in respect of the Additional Insurances.

The Insurances shall be:

maintained in accordance with Good Industry Practice;

(so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

maintained for at least six (6) years after the End Date.

The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

How to manage the insurance

Without limiting the other provisions of this Contract, the Supplier shall:

take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

What happens if you aren't insured

The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which

UK OFFICIAL

would entitle any insurer to refuse to pay any claim under any of the Insurances.

Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

Evidence of insurance you must provide

The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

Making sure you are insured to the required amount

The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

Cancelled Insurance

The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

Insurance claims

The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 0 relating to or arising out of the provision of the Deliverables

UK OFFICIAL

or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

UK OFFICIAL

ANNEX: REQUIRED INSURANCES

ANNEX 1 The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:

professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots ;

public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots;

employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000) – all Lots

product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots

UK OFFICIAL

Joint Schedule 4 (Commercially Sensitive Information)

What is the Commercially Sensitive Information?

In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	05/05/2023	Unit Pricing	Duration of the contract
2	05/05/2023	Configuration	Duration of the contract

Joint Schedule 6 (Key Subcontractors)

Restrictions on certain subcontractors

The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 0. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 20 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

- the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
- the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
- the proposed Key Subcontractor employs unfit persons.

The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

- the proposed Key Subcontractor’s name, registered office and company registration number;
- the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
- where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;
- for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
- for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
- the Dun & Bradstreet Failure Rating score of the Key Subcontractor.

If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 0, the Supplier shall also provide:

a copy of the proposed Key Sub-Contract; and

any further information reasonably requested by CCS and/or the Buyer.

The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

provisions which will enable the Supplier to discharge its obligations under the Contracts;

a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

the data protection requirements set out in Clause 14 (Data protection);

the FOIA and other access request requirements set out in Clause 16 (When you can share information);

the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

the conduct of audits set out in Clause 6 (Record keeping and reporting);

provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and

a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[**Guidance:** Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			

UK OFFICIAL

Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

UK OFFICIAL

Joint Schedule 11 (Processing Data)

Status of the Controller

- The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:
    - "Controller" in respect of the other Party who is "Processor";
    - "Processor" in respect of the other Party who is "Controller";
    - "Joint Controller" with the other Party;
    - "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

- Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
- The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
    - a systematic description of the envisaged Processing and the purpose of the Processing;
    - an assessment of the necessity and proportionality of the Processing in relation to the Services;
    - an assessment of the risks to the rights and freedoms of Data Subjects; and
    - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

- Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;
- ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
    - nature of the data to be protected;
    - harm that might result from a Data Loss Event;
    - state of technological development; and
    - cost of implementing any measures;
- ensure that :
    - the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
    - it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
        - are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
        - are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
        - are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
        - have undergone adequate training in the use, care, protection and handling of Personal Data;
- not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
- the Data Subject has enforceable rights and effective legal remedies;
- the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
- the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

▪ at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

○ Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

▪ receives a Data Subject Access Request (or purported Data Subject Access Request);

▪ receives a request to rectify, block or erase any Personal Data;

▪ receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

▪ receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

▪ receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

▪ becomes aware of a Data Loss Event.

○ The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.

○ Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this

Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- the Controller with full details and copies of the complaint, communication or request;
- such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
- the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- assistance as requested by the Controller following any Data Loss Event; and/or
- assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

- The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
  - the Controller determines that the Processing is not occasional;
  - the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
  - the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

- The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

- The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

- Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
  - notify the Controller in writing of the intended Subprocessor and Processing;
  - obtain the written consent of the Controller;
  - enter into a written agreement with the Subprocessor which gives effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

- provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

- The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

- The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

- The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

- In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

- With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

- Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

- Where a Party has provided Personal Data to the other Party in accordance with paragraph 17 of this Joint Schedule 11, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

- The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

- The Parties shall only provide Personal Data to each other:

- to the extent necessary to perform their respective obligations under the Contract;

- in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

- where it has recorded it in Annex 1 *(Processing Personal Data).*

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

- A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

- Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

  - the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

  - where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

    - promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

- provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

- Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

  - do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

  - implement any measures necessary to restore the security of any compromised Personal Data;

  - work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

  - not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

- Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

- Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

- Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data – N/A Replaced by Appendix 3

UK OFFICIAL

Framework Schedule 6

Call-Off Schedule 4 (Call Off Tender)

ISO 27001 - UK ONLY.pdf

001-PROJ1.1.docx to Have Declariation Fina am

06 PROJ1.4a Nice

05 PROJ1.3a Must Have Declariation

002-PROJ1.2.docx

03 DDaT22536. AW5.2 Rate Card.xls

MANDATORY CHARGE 5	
YEAR ONE	
[redacted]	
Total	**£176,160.88**
YEAR TWO	
[redacted]	
Total	**£139,910.00**
YEAR THREE	
[redacted]	
Total	**£139,910.00**
TOTAL CONTRACT VALUE	
Total	**£455,980.88**

UK OFFICIAL

Framework Schedule 6

Call-Off Schedule 5 (Pricing Details)

MANDATORY CHARGES	
YEAR ONE	
[redacted]	
Total	**£176,160.88**
YEAR TWO	
[redacted]	
Total	**£139,910.00**
YEAR THREE	
[redacted]	
Total	**£139,910.00**
TOTAL CONTRACT VALUE	
Total	**£455,980.88**

03 DDaT22536. AW5.2 Rate Card.xls

Call-Off Schedule 7 (Key Supplier Staff)

1. The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

    1. requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
    2. the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
    3. the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

5. The Supplier shall:
    1. notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
    2. ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
    3. give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least **three (3) Months '** notice;
    4. ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

5. ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

6. The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

UK OFFICIAL

Annex 1- Key Roles

Key Role	Key Staff	Contract Details
Senior Analyst	[redacted]	
IT Security Manager		
Head of Engineering		
SIAM		
Project Manager		
Insight internal AM		
Insight internal AM		
Insight external AM		
ANSecurity AM		

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Part A : Long Form Business Continuity and Disaster Recovery

1. Definitions

a. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"BCDR Plan" has the meaning given to it in Paragraph 2.2 of this Schedule;

"Business Continuity Plan" has the meaning given to it in Paragraph 2.3.2 of Part A of this Schedule

"Disaster Recovery Deliverables" the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;

"Disaster Recovery Plan" has the meaning given to it in Paragraph 2.3.3 of Part A of this Schedule

"Disaster Recovery System" the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;

"Related Supplier" any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;

"Review Report" has the meaning given to it in Paragraph 6.3 of Part A of this Schedule; and

"Supplier's Proposals" has the meaning given to it in Paragraph 6.3 of Part A of this Schedule;

2. BCDR Plan

a. The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

b. No more than **ninety (90**) Working Days after to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

i. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

ii. the recovery of the Deliverables in the event of a Disaster

c. The BCDR Plan shall be divided into three sections:

i. Section 1 which shall set out general principles applicable to the BCDR Plan;

ii. Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

iii. Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

d. Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

a. Section 1 of the BCDR Plan shall:

i. set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

ii. provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

iii. contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

iv. detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

v. contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

vi. contain a risk analysis, including:

1. failure or disruption scenarios and assessments of likely frequency of occurrence;
2. identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
3. identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
4. a business impact analysis of different anticipated failures or disruptions;

vii. provide for documentation of processes, including business processes, and procedures;

viii. set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

ix. identify the procedures for reverting to "normal service";

x. set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

xi. identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

xii. provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

b. The BCDR Plan shall be designed so as to ensure that:

i. the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

ii. the adverse impact of any Disaster is minimised as far as reasonably possible;

iii. it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

iv. it details a process for the management of disaster recovery testing.

c. The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

d. The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

a. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

i. the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

ii. the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

b. The Business Continuity Plan shall:

i. address the various possible levels of failures of or disruptions to the provision of Deliverables;

ii. set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

iii. specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

iv. set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

a. The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

b. The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

i. loss of access to the Buyer Premises;

ii. loss of utilities to the Buyer Premises;

iii. loss of the Supplier's helpdesk or CAFM system;

iv. loss of a Subcontractor;

v. emergency notification and escalation process;

vi. contact lists;

vii. staff training and awareness;

viii. BCDR Plan testing;

ix. post implementation review process;

x. any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

xi. details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

xii. access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

xiii. testing and management arrangements.

6. Review and changing the BCDR Plan

a. The Supplier shall review the BCDR Plan:

i. on a regular basis and as a minimum once every six (6) Months;

ii. within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

iii. where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its

review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

b. Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

c. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

d. Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

e. The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

a. The Supplier shall test the BCDR Plan:

   i. regularly and in any event not less than once in every Contract Year;

   ii. in the event of any major reconfiguration of the Deliverables

   iii. at any time where the Buyer considers it necessary (acting in its sole discretion).

b. If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

c. The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

d. The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

e. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

   i. the outcome of the test;

   ii. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

   iii. the Supplier's proposals for remedying any such failures.

f. Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

a. In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

a. The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

UK OFFICIAL

Call-Off Schedule 11 (Installation Works)

1. When this Schedule should be used

1.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of Deliverables requiring installation by the Supplier.

2. How things must be installed

2.1. Where the Supplier reasonably believes, it has completed the Installation Works it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:

2.1.1. accept the Installation Works, or

2.1.2. reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).

2.2. If the Buyer rejects the Installation Works in accordance with Paragraph 2.1.2, the Supplier shall immediately rectify or remedy any defects and if, in the Buyer's reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.

2.3. The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.1.1 Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.1, the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

2.4. Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

Framework Schedule 6

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Replacement of UKSBS SIEM
Duration of Contract including options for extension: 2 Years with an optional extension for 1 year.
Required Commencement Date: 30th May 2023

Introduction

1. The Security Information and Event Management (SIEM) service is used by the Risk, Information & Security Compliance (RISC) team to identify, log, and respond to activity that may pose a security threat to the business and maintain UKSBS ISO 27001 and Cyber Essentials certification.

2. The current SIEM Solution is hosted on premises within two virtual servers and one physical server which reaching its end-of-life date in 2023. The approaching end-of-life date mandates the upgrade or replacement of the UK SBS SIEM service by August of 2023.

3. Additionally, a recent disaster recovery review has highlighted that there is no equivalent service in the Rutherford Appleton Laboratory (RAL) which means that UK SBS would be unable to run this service in a disaster recovery (DR) situation.

4. The approaching end-of-life date mandates the upgrade or replacement of the UK SBS SIEM service by August of 2023. UK SBS should also take this opportunity to future proof the SIEM solution and create additional disaster recovery capability.

5. The current SIEM supplier have stated they intend to discontinue their on-premises solution soon and move to a cloud. This means that there is no path to continue the current on-premises solution.

6. To consider a replacement of the SIEM service at this critical time, with delivery of projects (SHARP and the MATRIX projects[1]), also add to the need to move to a cloud based SIEM service which is also in line with current industry trends.

Aims & Objectives

1. To migrate the current on-premises SIEM service to a cloud service.

2. Minimise the disruption to the monitoring of IT Services, Network and infrastructure at crucial time of moving enterprise systems to the cloud and to be ready for future requirements.

3. To provide coverage of the DR systems as well as Polaris House (PH) systems, AWS, and Azure domains.

4. Reduce the operational complexities of an on-premises solution i.e., maintenance of servers, patching vulnerabilities, application upgrades.

5. Reduce the risk of noncompliance with regulations.

6. Ease of configure and consumption of logs from RAL to a cloud service, which enables resilience for monitoring.

[1] Replacement ERP services for UKRI and UK Government.

7. Solution should be implemented before SHARP; this option should simplify the migration to Oracle Fusion because communicating of activity logs between two cloud services is easier than pulling logs to an on-premises service.

8. Freeing up of the infrastructure overheads that will no longer be required to maintain the on-premises hardware for the SIEM.

9. Legal and compliance considerations

    1. The inclusion of RAL networks in the cloud solution will meet the requirements for disaster recovery (DR).

    2. Activity logs captured by SIEM are only stored on the cloud for 90 days. UK SBS will need to purchase additional cloud storage to accommodate longer mandatory retention periods.

Objectives

3. To maintain the Security the UKSBS estate that is being monitored
4. To identify suspicious activities to enable UKSBS to respond in a timely manner.
5. This includes cloud services and DR capabilities.
6. The system must be resilient to support business continuity measures.
7. To Maintain ISO27001 and Cyber Essentials Certification

Background to the Requirement

The current SIEM Service was procured around 2012 initially to cover the monitoring of UKSBS managed systems hosted in Polaris House.

Disaster Recover (DR) was not considered at the time but should have been to ensure the resilience of the monitoring. This is now a requirement of future upgrades and replacement.

The system is continually evolving with the changes in technology, environments we operate and to the business need in response to Cyber Threats.

Current SIEM trends are to move towards cloud services, enabling customers to take better advantage of robust processing infrastructures.

It is a requirement of regulations such has ISO27001 and cyber essentials, that we monitor effectively, system access, user activities, system activities and application events. All this data must be processed by a SIEM to interpret the security of our estate.

The system is primarily monitored by the IT Security Team and the SOC analysts in D&I, with dashboards for specific functions.

Scope

1. Disaster Recovery for consideration to be included in the SIEM solution.
2. SIEM cloud solutions only to future proof UKSBS infrastructure.

3. Identify any 3rd party cost that enable the SIEM solution to fully interact with recognised applications (office 365 sevice now etc)
4. It is a requirement under ISO 27001 and Cyber Essentials to have an effective SIEM monitoring platform
5. There is current DPIA in place which will be revised to cover the adoption of a cloud SIEM Solution.

Requirement

Must Have

6. Cloud SIEM service covering Polaris House and RAL networks and integrate with log collection loud services in AWS, Azure and Oracle.
7. The solution must provide a highly available redundant system.
8. The solution must alert/alarm with risk-based prioritisation related to the detection and behaviour.
9. The solution must be able to receive logs from multiple locations (Main site and DR site).
10. Provide capability for Logs to be normalised and time chronicled upon ingestion.
11. The ingested logs aligned to a common schema at point of ingestion.
12. No significant changes to the overall design of the monitoring solution; effectively it is enabling the SIEM servers in the cloud.
13. The solution must use an Artificial Intelligence Engine.
14. The solution must be able to utilise modern technologies, such as APIs, Machine Learning and Security Orchestration, Automation and Response.
15. The solution must provide multiple methods for collecting log data (i.e. agents, directly via network protocol/API, accessing logs from storage).
16. The solution must be able to centralise all security notifications from all UK SBS technologies: firewalls, IDS/IPS systems, AV consoles, wireless access points, AD servers, etc. with one set of reports within one centralised system for generating notifications.
17. The solution must be accessible from modern browsers such as Edge, Chrome including mobile browsers.
18. The solution must provide end to end encryption for transportation of logs.
19. The solution must provide adequate storage for log retention, which adheres to UK SBS policies (13 months), and provides the ability to search historical events.
20. The solution must provide preconfigured rules and have the capability to quickly develop new rules.
21. The solution must provide preconfigured dashboards and capability to develop dashboards to reflect overall status of the infrastructure.
22. The solution must reduce mean time to detect (MTTD) and mean time to respond (MTTR) through a full set of analytics.
23. The solution must be able to accept/parse multiple log formats and allow custom parsing.
24. The solution must adequately support current event volume(s) and scale for projected growth.
25. The solution must incorporate threat intelligence feeds from multiple sources, with capabilities to allow custom threat feeds
26. The solution must allow querying of data, to allow exploration of the data to hunt for threats.
27. The ability to export logs for external investigation.

28. The Approved SIEM must have a training program in place to teach current and future security personnel.
29. The ability to ingest logs and configuration from current SIEM in full.
30. Detailed deployment plan for new solution showing how the SIEM product will connect to all existing services.
31. It must have reporting capabilities out-of-the-box, and customisable reporting.
32. have capabilities for potential future requirements for integrated UEBA, integrated NDR and integrated File integrity monitoring and Registry integrity monitoring.

Nice to Have

33. Clearly defined escalation process.
34. The SIEM cloud solution should be easily deployable onto the existing UKSBS network, enabling all existing tools and applications to connect and report to the SIEM solution.
35. The Stored data should be optimised and indexed for efficient analysis and exploration.
36. There should be a clear process for escalation of support issues.
37. The management console should be intuitively designed and customisable.

Timetable

1. Current contract finishes in August 2023. The replacement SIEM must work in parallel with existing system until proven and covers the entire systems to be monitored.
2. Target to replace the current SIEM Service on Premise system with a cloud version will take one month. This means the replacement must be in place for 30 Jun 2023 to start the hand over and to allow contingency.
3. Target to replace the Current SIEM service with a new supplier 18 to 24 Months requiring the extension of the current SIEM service, this raises other technical issues.
4. It is desirable that the cloud service is in place before SHARP goes live, which is end of July 2023. If not available will cause the need to run current system past its end of life.
5. It is a must for MATRIX continual support when it goes live.

Key Milestones

Milestone/Deliverable	Description	Timeframe or Delivery Date
Installation	To run parallel with existing system to confirm usability and functionality	30/06/2023
Test	Dual running of the installation to ensure we are seeing the same results	30/06/2023
Transfer	Transfer of service must be complete.	31/08/2023

UK OFFICIAL

Appendix 1 (Supplier Statement of Works)

LogRhythm

UKSBS

Shared Business Services

UKSBS Cloud Migration
Statement of Work

Date: Mar 23, 2023

UK OFFICIAL

Framework Schedule 6

UKSBS Cloud Migration Statement of Work

Table of Contents

UK OFFICIAL

Table of Figures

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

THIS STATEMENT OF WORK ("SOW") is hereby entered into as of, March 23, 2023 ("SOW Effective Date") between LogRhythm Inc. ("LogRhythm") and UKSBS Cloud Migration ("Customer"). This Statement of Work ("SOW") is governed by the LogRhythm End User License Agreement the following location: https://gallery.logrhythm.com/terms-and-conditions/LOGRHYTHM-GLOBAL-END-USER-LICENSE-AGREEMENT-03-2021.pdf. Except that if Customer has signed Terms and Conditions ("Agreement") with LogRhythm, this SOW will be governed by the Agreement. This SOW includes the Appendices attached hereto.

1 Effort Estimate of Services

LogRhythm will provide the Services set forth in the Quote or the quote provided by LogRhythm's partner ("Quote") and as defined in Section 2 of this document, Description of Services. The Quote and the table below specify the estimated number of consulting days of Services which will be provided under this SOW. For purposes of this SOW, if time is specified in days, one (1) consulting day is eight (8) hours, inclusive of one (1) hour to cover breaks.

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

2 Description of Services

LogRhythm will provide consulting and technical expertise to deliver the work defined in this SOW, not to exceed the Total Estimated Effort detailed in Table 1 above. This Statement of Work is structured as a time and materials engagement. As such, all effort estimates listed in Table 1 are produced in good faith and do not guarantee scope completion. Unless otherwise specified, all Services will be performed remotely.

As it pertains to the scope defined in the remainder of Section 2, billable activities include, but are not limited to, design, implementation, testing, documentation, meetings (preparation, participation, and follow-up), project management, phone calls, emails, status updates, and knowledge transfer.

2.1 Project Management

LogRhythm will perform the following project management tasks. Depending on the size and scope of the project, these tasks may be performed by a Project Manager, Project Coordinator or the lead Technical consultant.

2.1.1 Activities Performed

1. Be the overall focal point for the project.
2. Work with Customer's project manager or single point of contact to review the project scope, define success criteria, create the project schedule, and review the implementation process including Customer tasks and deliverables.
3. Hold a pre-deployment meeting via conference call that will include the following activities:
    a. Review the purchased scope of work
    b. Explain the project approach
    c. Confirm Customer's overall objectives of the project
    d. Review the required Customer participation, tasks, and deliverables
    e. Discuss the preliminary deployment schedule
4. Hold periodic progress meetings and provide written status reports, including a summary of hours billed to the project.
5. If required, develop a Deployment Plan Document.

2.1.2 Customer Responsibilities

1. Assign a person (e.g. project manager) to coordinate with LogRhythm on all aspects of the project planning and deployment.
2. Organize and assemble the appropriate Customer resources to assist LogRhythm throughout the project.

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

2.2 Migration

LogRhythm will migrate the SIEM solution to a new host(s).

2.2.1 Activities Performed

1. Migrate SIEM to new hardware.
2. Apply LogRhythm recommended configurations and best practices for the software version installed.
3. Conduct product overview knowledge transfer throughout the engagement.
4. Validate the system functions as designed.

2.2.2 Customer Responsibilities

Prior to the deployment review phase starting, Customer will complete the following tasks:

1. Receive and rack server(s) (hardware deployments only).
2. Deploy and configure virtual servers per LogRhythm specifications (software deployments only).
3. Power on server(s) and perform initial operating system configuration when prompted.
4. Assign static IP address(es).
5. Assign a host name.
6. Ensure RDP/SSH access.
7. Ensure access and permission to install on Windows/Linux host(s).
8. Configure antivirus exclusions.
1. Open relevant firewall ports.
2. Create/provide service accounts required for solution.
3. Ensure any required change control approvals are in place.

2.2.3 Deliverables

1. All core software components installed and configured per the upgrade guide and best practice.
2. Deployment configuration signoff.

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

2.3 Upgrade

LogRhythm will upgrade the SIEM solution to the latest "general available" (GA) release.

2.3.1 Activities Performed

1. Upgrade the SIEM software version to the latest GA release.
2. Apply LogRhythm recommended configurations and best practices for the software version installed.
3. Conduct product overview knowledge transfer throughout the engagement.
4. Validate the system functions as designed.

2.3.2 Customer Responsibilities

Prior to the deployment review phase starting, Customer will complete the following tasks:

1. Ensure RDP/SSH access.
2. Ensure access and permission to install on Windows/Linux host(s).
3. Configure antivirus exclusions.
4. Open relevant firewall ports.
5. Create/provide service accounts required for solution.
6. Ensure any required change control approvals are in place.

2.3.3 Deliverables

1. All core software components installed and configured per the upgrade guide and best practice.
2. Deployment configuration signoff.

2.4 Ad Hoc Consulting Time

This is an allotment of hours as specified in Table 1 that can be used at the discretion of Customer. A LogRhythm consultant will perform these activities as directed by Customer as long as there are unused Ad Hoc hours that have been purchased or transferred from other scope in this SOW.

As this is a time and materials SOW, any remaining capacity from the scope defined in Section 2 and Table 1 will automatically be rolled into Ad Hoc Consulting Time and adhere to these terms without a Change Order.

2.4.1 Activities Performed

1. Activities to be defined by Customer and agreed upon by LogRhythm project management.

2.4.2 Customer Responsibilities

1. Define tasks to be performed.

2.4.3 Deliverables

1. Completion of the Customer-defined task(s) as agreed upon by LogRhythm project management.

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

3 General Assumptions

The Scope of Work and effort estimates defined in this document are based on the following assumptions. If any of the assumptions change or prove to be false, additional fees may apply.

Customer will provide reasonable cooperation to LogRhythm in its performance of the services outlined in this Statement of Work.

1. Any work that is not specifically set forth in this SOW is out of scope and would require an additional SOW or change request to the existing SOW. The addition of Services via an additional SOW or change request may incur additional fees.

2. Unless otherwise specified, the Services outlined in this SOW will be performed remotely by LogRhythm. For these Services, Customer will provide LogRhythm remote access to the Customer LogRhythm platform and Customer network for the duration of the project. LogRhythm employees will comply with all Customer network security standards.

3. Customer will provide a single point of contact for the duration of the project.

4. Depending on the task, participation from the following Customer roles may be required:
    - SIEM Administrator
    - SOC Analyst/Manager
    - Security Manager
    - Log Source Owners
    - Compliance Representative

5. LogRhythm will be reliant on Customer's staff to complete identified tasks and provide information in a timely manner. Any delay in Customer's ability to complete these tasks and/or provide any requested information may affect the completion of the overall project tasks and deliverables.

6. In scope firewall and network obstruction points are known.

7. LogRhythm will consider all Customer information and documentation as sensitive and confidential and will handle appropriately.

8. Deliverables will be reviewed by Customer and returned with comments within 10 business days of delivery. Acceptance of the deliverable will be assumed if no comments are received from Customer during that time.

9. If Customer has purchased hardware from LogRhythm or another vendor, Customer is responsible for racking and cabling hardware unless explicitly delegated to LogRhythm or Partner resources in this Statement of Work.

10. If Customer is deploying to a virtual environment, all prerequisites and specifications outline in the LogRhythm Software Install guide will be met before the start of any deployment work.

11. The deployment Consultant will not be responsible for the configuration of any application other than the LogRhythm SIEM or Network Monitor solutions during the deployment.

12. Customer will provide a member of their support team to assist the deployment Consultant when required.

13. Any network environment issues which arise outside of the deployment activities are the responsibility of Customer. Any issues which impact the deployment timelines must be resolved by Customer within agreed timeframes so as to limit the impact on the deployment.

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

4 Scheduling Authority for Professional Services

The Services will be coordinated with Customer's Project Lead. Customer may appoint in writing (email) additional representatives to act on Customer's behalf.

4.1 Work Scheduling

Services will generally be performed during normal business hours as defined below, Customer local time, excluding LogRhythm corporate holidays. Work performed after-hours on weekdays will be charged at a rate of 1.5 hours per hour worked. For work performed on weekends, 2 hours will be billed per hour worked. If onsite Services are requested, the duration may not be less than three days.

Normal business hours by region:

- North and South America: Monday – Friday 8 AM – 5 PM
- Europe, Asia, India, and Australia: Monday – Friday 9 AM – 5 PM
- Middle East: Sunday – Thursday 9 AM – 5 PM

4.2 Professional Services Cancellation Policy

- **Customer On-Site Services**: all requests for cancellations of scheduled Services that are to be delivered on a Customer's site must be received at least one (1) business week in advance of the time the Services are scheduled to begin. If a cancellation is made less than one (1) business week prior to the start of the scheduled session, LogRhythm will make reasonable attempts to fill the allotted consultant time with other customer engagements. If LogRhythm does not fill the allotted time, then the Customer's Services hours will be decremented in the amount of one working day (8 hours) and Customer will reimburse LogRhythm for any actual non-cancellable travel and accommodation expenses.

- **Remote Services**: all requests for cancellations of scheduled Services that are to be delivered remotely must be received at least 2 business days in advance of the time the service is scheduled to begin. If the cancellation is made fewer than 2 business days prior to the start of the scheduled session, LogRhythm will make reasonable attempts to fill the allotted consultant time with other customer engagements. If LogRhythm does not fill the allotted time, then Customer's Services hours will be decremented in the amount of the pre-scheduled Services hours, up to a maximum of 8 hours.

- To cancel a session, Customer will contact the appropriate LogRhythm Project Management team.
    - North and South America: projectmgmt@logrhythm.com
    - Europe, Middle East, and India: projectmgmt.emea@logrhythm.com
    - Asia and Australia: projectmgmt.apj@logrhythm.com

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

5 Change Request Process

Either party may request changes to this SOW. Any changes to this SOW will be documented by LogRhythm on a Change Request form, which will include a description of the change and its impact on the project, including any impact on costs / charges and schedule. All parties will evaluate the change for approval. Any such changes will not be effective until a Change Request form reflecting the changes has been created, agreed upon and signed by the parties.

The execution of the Change Request Form by both parties will cause the Change Request Form to become part of and incorporated into this SOW. Commencement of the performance of the requested change is conditioned upon the mutual execution of the Change Request, and LogRhythm's receipt of an additional P.O. authorization to cover the agreed upon price for each requested change.

6 Fees and Expenses

Unless tasks are otherwise specified as "Fixed Fee" in Table 1, Purchased Professional Services, all Services are performed as Time and Materials and sold as "Professional Services Days". Professional Service Days are valid for a period of one year from the purchase date. Per the End User License Agreement, LogRhythm reserves the right to expire any remaining days not used within the one-year timeframe at which point the expired days will be unavailable for use beyond the one-year timeframe.

6.1 Payment Terms

All Services fees are invoiced in accordance with the Quote and are payable according to the Agreement.

OR

The fees for Services set forth in this SOW are as quoted between Customer and Reseller/Distributor.

6.2 Travel Expenses

If travel to a Customer location is required, travel can be prepaid in advance or a Change Order will be executed against this SOW as agreed upon by LogRhythm and Customer or Partner project management. Unless otherwise agreed to, all travel arrangements will be made in accordance with the LogRhythm travel policy.

UK OFFICIAL

Framework Schedule 6

UKSBS Cloud Migration Statement of Work

7 Acceptance

The completion of this Scope of Work will be deemed accepted when:

- LogRhythm provides documentation stating all deliverables specified in this SOW are complete
- Customer agrees in writing that all deliverables specified in this SOW have been complete OR LogRhythm receives no written notice of rejection within ten (10) business days of submitting written confirmation of SOW completion.

8 Customer Signature Block

UK OFFICIAL

Framework Schedule 6

UKSBS Cloud Migration Statement of Work

9 Appendix A: Assumptions

The list of assumptions below was used to develop this Scope of Work and the effort estimate. If any of the assumptions change or are incorrect, additional charges may apply.

Table 2: Effort Estimation Assumptions

Information	Value
Global Assumptions	[redacted]
Remote or On-site Deployment	
# of Trips	
Security Clearance Required?	
Solution Overview and Sizing	
Sustained Messages Per Second Volume (K)	
Peak Messages Per Second Volume (K)	
Data Indexer Indexing Profile	
Data Indexer Time-to-Live (days)	
Average Log Size (bytes)	
SIEM	
Current Existing SIEM Solution	
HW, SW, or LR Cloud Installation	
Appliance Quantity (total number of XM, PM, DP, AIE, DC, SA)	
# of DX Clusters	
Migration	
Migration Required?	
HW, SW or LR Cloud Installation	
Brief Description	
Upgrade	
Upgrade?	
Current SIEM Version	
Target SIEM Version	
Windows OS Upgrade Required?	
Project Management	
Project Management (%)	

UK OFFICIAL

Framework Schedule 6

UKSBS Cloud Migration Statement of Work

10 Appendix B: Change Request Form

LogRhythm

Change Request Number: [#####]
Change Submittal Date: [##-##-##]

Requestor

Request Originator [LogRhythm / Customer]

Cost/Price Impact: _____

Schedule Impact: _____

Terms Impact: ☐ No ☐ Yes (Describe terms change in description below)

Description of SOW Change

(Attach additional pages as necessary)

Change Request Approval

Approval of this Change Request, as written, is affirmed by the signatures of the duly authorized representatives of the parties below:

LogRhythm, Inc		UKSBS Cloud Migration	
Signature	Date	Signature	Date
Name		Name	
Title		Title	

For LR Internal use only: P.O. Required? ☐ No ☐ Yes P.O. Received? ☐ No ☐ Yes

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

11 Appendix B: Abbreviations

Table 3: Abbreviations

Abbreviation	Description
AD	Active Directory
AES	Advanced Encryption Standard
AHC	Automatic Host Contextualisation
AIE	Advance Intelligence Engine
AIEDP	Advance Intelligence Engine Data Provider
AIEDR	Advance Intelligence Engine Data Receiver
APT	Advance Persistent Threat
ARM	Alarm and Response Manager
CAL	Client Access License
CC	Common Criteria
CN	Common Name
DC	Data Collector
DLD	Data Loss Defender
DN	Data Node
DNS	Domain Name System
DP	Data Processor
DR	Disaster Recovery
DX	Data Indexer
DXW	Data Indexer Warm Node
EAL	Evaluation Assurance Level
EDF	Environmental Dependence Factor
EMDB	Platform Manager Database
FIM	File Integrity Monitor
FIPS	Federal Information Processing Standards
FPP	False Positive Probability
GLPR	Global Log Processing Rule
HA	High Availability
HIDS	Host Intrusion Detection System
HW	Hardware
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
KB	Knowledge Base
LDS	Log Distribution Services
LR	LogRhythm
MCF	Milestone Completion Form
MIB	Management Information Base
MPS	Messages Per Second
MTTD	Mean-Time-to-Detect
MTTR	Mean-Time-to-Respond
NAT	Network Address Translation
NDR	Network Detection and Response
NetMon	Network Monitor
NIC	Network Interface Controller
NOC	Network Operations Centre
NTBA	Network Traffic and Behavior Analytics
OS	Operating System
PDU	Power Distribution Unit
PII	Personally Identifiable Information
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PM	Platform Manager

UK OFFICIAL

UKSBS Cloud Migration Statement of Work

PSU	Power Supply Unit
PS	Professional Services
RADB	Restore Archive Database
RAID	Redundant Array of Independent Disks
RBP	Risk Based Priority
RR	Risk Rating
SA	Storage Array
SDEE	Security Device Event Exchange
SIEM	Security Information & Event Management
SMA	System Monitor Agent
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
SOMM	Security Operations Maturity Model
SOW	Statement of Work
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guides
SW	Software
TCP	Transmission Control Protocol
TFC	Trace File Converter
TLM	Threat Lifecycle Management
TMF	Threat Management Foundations
TLS	Transport Layer Security
TMF	Threat Management Foundations
TTL	Time-to-Live
UAM	User Activity Monitor
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UDLA	Universal Database Log Adapter
UEBA	User and Entity Behaviour Analytics
UTC	Coordinate Universal Time
VMID	Vendor Message ID
XM	LogRhythm Server which includes a Platform Manager (PM) and Data Processor (DP)

In the event of any conflict the terms of this Call-off Contract take precedence over the terms outlined under the SoW.

UK OFFICIAL

Framework Schedule 6

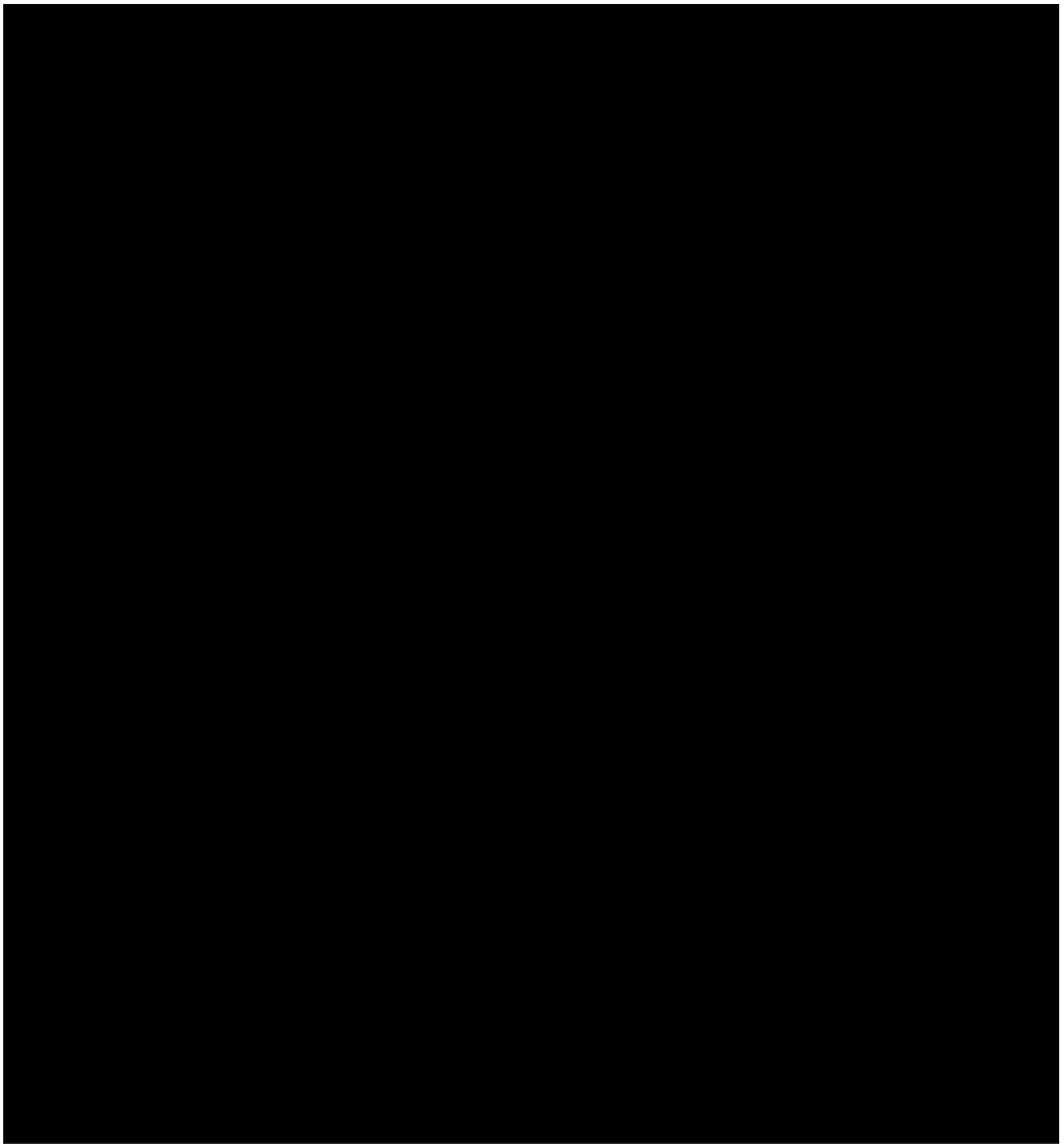
Appendix 2 (Information Security)

ISO 27001 - UK ONLY.pdf

[redacted]

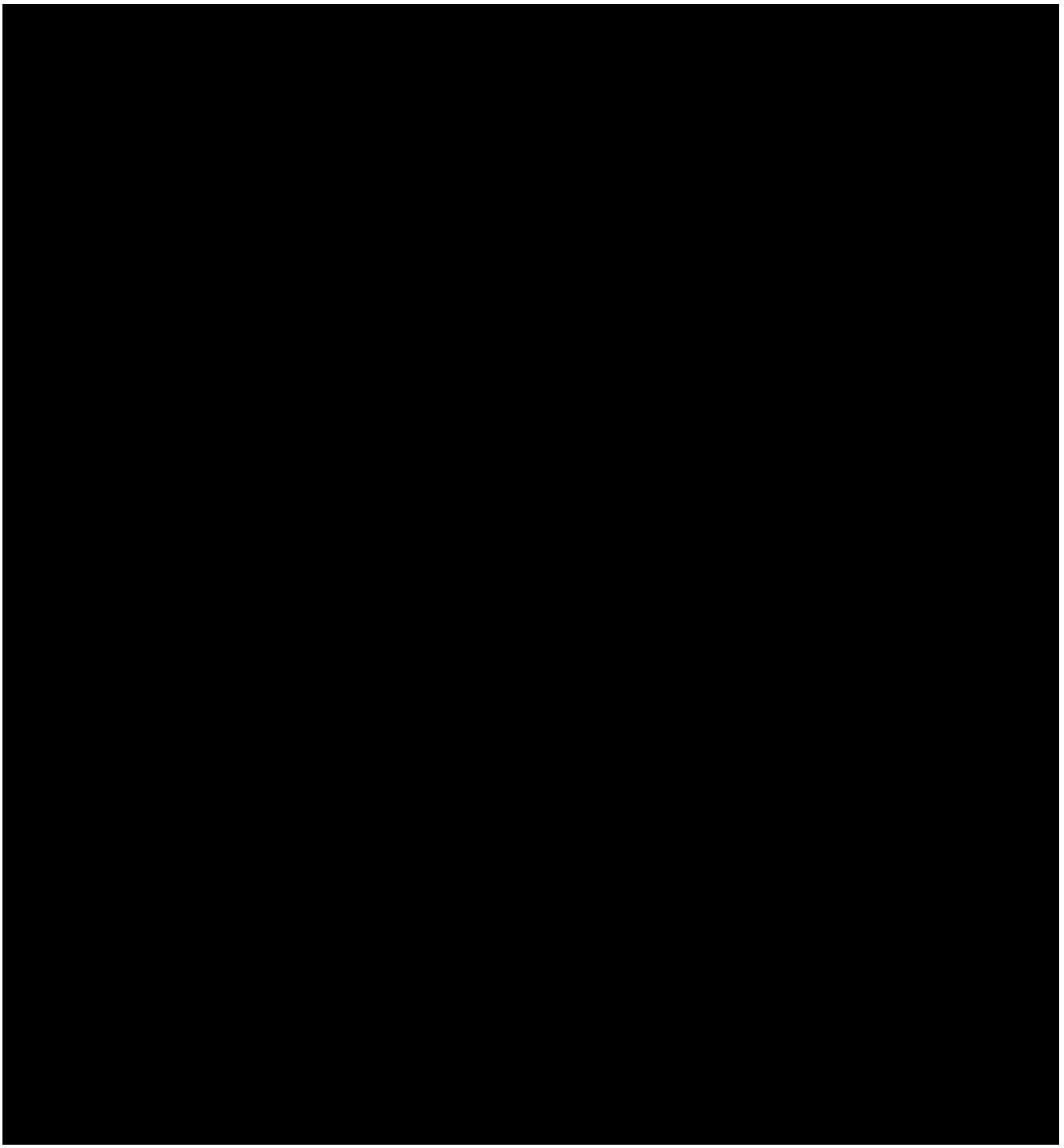
UK OFFICIAL

Framework Schedule 6



UK OFFICIAL

Framework Schedule 6



UK OFFICIAL

Appendix 3 (DPIA)

LogRhythm: EMEA Data Processing Agreement

This Data Processing Agreement (***"DPA"***) is incorporated by reference into the LogRhythm Software as a Service Agreement (***"Agreement"***) between the customer named below (***"Customer"***) and the LogRhythm entity who is a party to the Agreement (***"LogRhythm"***).

This DPA is entered into as of the later of the dates beneath the parties' signatures below.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable EU+ Data Protection Legislation, in the name and on behalf of its Authorized Affiliates (as defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

HOW TO EXECUTE THIS DPA

This

HOW THIS GDPR ADDENDUM APPLIES

5. If the Customer entity signing this DPA is a party to the Agreement, the LogRhythm entity that is a party to the Agreement is a party to this DPA.

6. If the Customer entity signing this DPA has executed orders for LogRhythm products or services under the Agreement but is not a party to the Agreement, this DPA will be incorporated in such order(s) and the LogRhythm entity that is a party to such order(s) is a party to this DPA.

7. If the Customer entity signing this DPA is lawfully permitting an Authorized Affiliate to use the Services, that Customer Affiliate is a party to this DPA.

DPA Terms

DEFINITIONS

Terms used in this DPA have the same meaning as those used in the Agreement, unless provided otherwise.

"*Affiliate*" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"***Authorized Affiliate***" means any of Customer's Affiliate(s) which (a) qualifies as a Controller or acts as a Processor on behalf of a third party in respect of relevant Personal Data, (b) is permitted to use the Services pursuant to the Agreement, and (c) on whose behalf LogRhythm Processes certain Personal Data under the Agreement.

"*Controller*" means the entity which determines the purposes and means of the Processing of Personal Data.

"*Data Subject*" means the individual to whom Personal Data relates.

"***EU+ Data Protection Legislation***" means the GDPR, together with applicable EU/EEA member state laws or UK laws implementing or supplementing the GDPR (including the UK Data Protection Act 2018 (as amended)).

"GDPR" means, as and where applicable: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the ***"EU GDPR"***); and/or (b) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (the ***"UK GDPR"***). References to ***"Articles"*** and ***"Chapters"*** of, and other relevant defined terms in, the GDPR shall be construed accordingly.

"*Personal Data*" means any personal data (as that term is defined in the GDPR) comprised within the Customer Data.

"*Processing*" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"*Processor*" means the entity which Processes Personal Data on behalf of the Controller.

"Relevant Body" means (a) in the context of the UK and the UK GDPR, the UK Information Commissioner's Office and/or UK Government (as and where applicable); and/or (b) in the context of the EEA and EU GDPR, the European Commission.

"Restricted Transfer" means the disclosure, grant of access or other transfer or transmission of Personal Data to any person in either: (a) in the context of the UK, a country or territory outside the UK ("***UK Restricted Transfer***"); and/or (b) in the context of the EEA, a country or territory outside the EEA ("***EU Restricted Transfer***"), which the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made or approved under Article 45 of the GDPR and which requires a 'transfer mechanism' under Chapter V to comply with the GDPR;

"*Services*" means the services provided by LogRhythm in relation to the Processing of Customer's Personal Data as described in the Agreement (as amended from time to time).

"SCCs" means the standard contractual clauses issued or approved from time-to-time by the Relevant Body for use in respect of Restricted Transfers to Processors, the current forms of which are attached hereto: (a) in respect of UK Restricted Transfers, as Schedule 2 ("***UK SCCs***"); and (b) in respect of EU Restricted Transfers, as Schedule 3 ("***EU SCCs***").

"*Sub-processor*" means any Processor engaged by LogRhythm to Process Personal Data as part of the Services.

"Supervisory Authority" (a) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office ; and (b) in the context of the EEA and EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

In case of any conflict or inconsistency between:

(a) this DPA and the Agreement, the provisions in this DPA shall prevail to the extent of such conflict or inconsistency; or

(b) any SCCs that may apply in accordance with Section 7.14 and/or 7.15 and this DPA and/or the Agreement, notwithstanding any "Operational Clarifications" detailed herein, those SCCs shall prevail in the context of the Restricted Transfer(s) to which they apply to the extent of any such conflict or inconsistency.

PROCESSING OF PERSONAL DATA

7.1 Roles of the Parties. Subject to Section 7.18, the Parties acknowledge that as between the Parties, Customer is a Controller and that LogRhythm is a Processor in connection with Processing of Personal Data carried out in performance of the Services. Each party shall comply with the obligations that apply to it under the EU+ Data Protection Legislation, having regard to the respective statuses described in the preceding sentence.

7.2 LogRhythm Processing of Personal Data. Subject to Section 7.18, LogRhythm shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and EU+ Data Protection Legislation.

7.3 Details of the Processing. The subject-matter of Processing of Personal Data by LogRhythm is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

SECURITY

7.4 Protection of Personal Data. LogRhythm shall implement appropriate technical and organisational measures taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. Such measures shall be designed to

ensure a level of security appropriate to the risk in order to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or use (each a ***"Security Incident"***) and in accordance with security standards as set forth in the Agreement. Without limiting the generality of the foregoing, LogRhythm shall comply with the security measures detailed in Schedule 4 ("***Security Measures***").

7.5 Incident Management - Notifications. Upon becoming aware of a Security Incident affecting Personal Data, transmitted, stored or otherwise Processed by LogRhythm or its Sub-processors, LogRhythm shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under and in accordance with the timescales required by the EU+ Data Protection Legislation. LogRhythm shall further take all such measures and actions as are necessary to remedy or mitigate the effects of such Security Incident and shall keep Customer informed of all developments in connection with such Security Incident.

7.6 Operational clarification relevant to the UK SCCs. The Parties agree that the provisions of Sections 7.4 to 7.5 satisfy applicable requirements of the UK SCCs.

SUBPROCESSING

7.7 Authorization. Customer generally authorizes LogRhythm to appoint Sub-processors. LogRhythm may continue to use those Sub-processors already engaged by LogRhythm as at the effective date of this DPA (as those Sub-processors are shown, together with their respective functions and locations, in [Schedule 5 (Authorized Sub-processors)] **OR** [the Sub-processor List shown at [INSERT PAGE]] (the "**Sub-processor List**")), the engagement of each of whom is hereby approved by Customer.

7.8 Responsibility. LogRhythm shall impose on such Sub-processors data protection terms that protect the Personal Data to the same standard provided for by this DPA and shall remain liable for any breach of this DPA caused by a Sub-processor.

7.9 Appointment and objection. When LogRhythm wishes to appoint a new Sub-processor to Process Personal Data hereunder, LogRhythm will notify Customer of the engagement at least [thirty (30) days] in advance (including providing the name and location of the relevant Sub-processor and the activities it will perform) [by providing Customer with an updated copy of the Sub-proc es s or Lis t v ia a ' mai ls hot ' or s im il ar mas s dis tr ibut io n mec h anis m s ent v ia ema il t o Cus tomer 's n orma l addres s ees for s y s tem upd ates]. In the event that Customer does not object to LogRhythm's use of a new Sub-processor in writing within such [thirty (30) day] period, Cus- tomer agrees that it shall be deemed to have approved the engagement and ongoing use of that Sub-processor. In the event Customer objects to a new Sub-processor, LogRhythm will use reasonable efforts to make available to Customer a change in the Services or recommend a change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If LogRhythm is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable order(s) with respect only to those Services which cannot be provided by LogRhythm without the use of the objected- to new Sub-processor by providing written notice to LogRhythm. LogRhythm will refund Cus- tomer any prepaid fees covering the remainder of the term of such Order(s) following the effec- tive date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer. This Section 7.9 set outs Customer's sole and exclusive remedy if Customer objects to any new Sub-processor.

7.10 Operational clarifications relevant to the SCCs:

(a) The terms and conditions of Sections 7.7 to 7.9 apply in relation to LogRhythm's appointment and use of Sub-processors under the SCCs.

(b) Any approval by Customer of LogRhythm's appointment of a Sub-processor that is given expressly or deemed given pursuant to Sections 7.7 or 7.9 constitutes Customer's: (i) prior written consent to LogRhythm's appointment of that Sub-processor if and as required under Clause 5(h) of the UK SCCs; and (ii) documented instructions to effect onwards transfers to any relevant Sub-processors if and as required under Clause 8.8 of the EU SCCs.

(c) LogRhythm will only provide copies of Sub-processor agreements to Customer under Clause 5(j) of the UK SCCs upon Customer's request; provided that, LogRhythm may remove or redact therefrom all commercial information and/or any clauses, recitals, schedules, annexes, appendices etc., unrelated to the UK SCCs beforehand.

ACCESS

7.11 Limited Access. LogRhythm shall limit access to the Personal Data to duly authorized officers, employees, agents and contractors ("**LogRhythm Personnel**") who need access to the Personal Data to meet LogRhythm's obligations under the Agreement and this DPA.

7.12 Confidentiality. LogRhythm shall ensure that all LogRhythm Personnel:

(a) are informed of the confidential nature of the Personal Data;

(b) have undertaken training in the care, protection and handling of personal data; and

(c) are aware of both LogRhythm's duties and their personal duties and obligations under the EU+ Data Protection Legislation and this DPA.

INTERNATIONAL TRANSFERS

7.13 Data transfers. The Parties acknowledge that Customer's transmission of Personal Data to LogRhythm hereunder may involve a UK Restricted Transfer and/or an EU Restricted Transfer. The relevant set(s) of SCCs that may be entered into under Section 7.14 and/or 7.15 shall apply and have effect only if and to the extent permitted and required under the EU GDPR and/or UK GDPR to establish a valid basis under Chapter V or the EU GDPR and/or UK GDPR (if and as applicable) in respect of the transfer to LogRhythm of Personal Data under this DPA.

7.14 EU Restricted Transfers To the extent that any Processing of Personal Data under this DPA involves an EU Restricted Transfer, the Parties shall comply with their respective obligations set out in the EU SCCs. The following modules of the EU SCCs apply in the manner set out below (having regard to the role of the Customer) –

(a) Module 2 of the EU SCCs applies to any EU Restricted Transfer involving Processing of Personal Data in respect of which Customer is a Controller in its own right; and/or

(b) Module 3 of the EU SCCs applies to any EU Restricted Transfer involving Processing of Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including Authorized Affiliates).

7.15 UK Restricted Transfers. To the extent that any Processing of Personal Data under this DPA involves a UK Restricted Transfer, the Parties shall comply with their respective obligations set out in the UK SCCs, which are hereby deemed entered into and incorporated by reference into this DPA.

7.16 UK Restricted Transfer-specific acknowledgements.

(a) In respect of any UK Restricted Transfer involving Processing in respect of which Customer is itself acting as a Processor on behalf of any other person (including Authorized Affiliates), Customer warrants and represents on an ongoing basis, and further undertakes, that it has full and sufficient authority to enter into the UK SCCs for and on behalf of each such other person.

(b) To the extent that LogRhythm effects an onwards transfer to a Sub-processor in respect of Personal Data to which the UK SCCs apply, Customer hereby authorizes LogRhythm to enter into the UK SCCs as agent for Customer (as 'data exporter') with that Sub-processor (as 'data importer'), which it may (at its option) elect to do in order to meet its obligations to Customer under Clause 11 of the UK SCCs.

7.17 Adoption of new SCCs. Notwithstanding the generality of Section 7.25, LogRhythm may on notice vary this DPA and replace the relevant SCCs with any new form of the relevant SCCs issued or approved by the Relevant Body(ies), which shall be suitably populated having regard to the relevant transfer to which such updated SCCs are to be applied.

USER BEHAVIOUR ANALYSIS

7.18 In connection with the provision of its services to its customers, LogRhythm may Process certain personal data (as defined in the GDPR) comprised within log-level / event-level records (such data ***"Analytics Data"***) for the purposes of analysing user-behaviour occurring on or in respect of its customers' networks and information technology systems (including identifying and analysing general usage or behavioural trends and patterns), which may be used to provide security-relevant information to LogRhythm's customers and/or otherwise to develop, enhance and/or improve its security services and the products and services it offers and provides to customers, including certain aggregation, anonymisation, de-identification or pseudonymisation of Analytics Data (***"User Behaviour Analysis"***).

7.19 LogRhythm acts as an independent Controller in respect of its Processing of any Analytics Data for the purposes of User Behaviour Analysis, and shall (a) comply with applicable EU+ Data Protection Legislation in respect of such Processing; (b) safeguard such Analytics Data with security measures that are no less protective than those required by this DPA; and (c) not disclose any Analytics Data that identifies Customer and/or any relevant Data Subjects to any third parties (other than its Affiliates and Processors) unless permitted under the Agreement and/or this DPA, and/or the disclosure is required in order to comply with applicable law.

7.20 Customer shall ensure that all relevant Data Subjects (including Customer's personnel) are made aware of LogRhythm's Processing for Analytics Data for the purposes of User Behaviour Analysis by providing such Data Subjects with a suitably prominent link to LogRhythm's privacy policy notified to Customer from time-to-time.

COOPERATION

7.21 Data Subjects' Rights. LogRhythm shall provide Customer with all assistance that it reasonably requires, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under EU+ Data Protection Legislation, including rights of access, correction, restriction, objection, erasure or data portability, as applicable. In the event such inquiry, communication or request is made directly to LogRhythm, LogRhythm shall promptly inform Customer by providing the full details of the request. For the avoidance

of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability involving that Data Subject's Personal Data.

7.22 Supervisory Authorities. LogRhythm shall notify Customer without undue delay if a Supervisory Authority or law enforcement authority makes any inquiry or request for disclosure regarding the LogRhythm's Processing of Personal Data, and shall provide Customer with reasonable assistance in respect thereof.

7.23 Cooperation with Customer. LogRhythm shall, to the extent required by EU+ Data Protection Legislation, provide Customer with reasonable assistance: (i) with data protection impact assessments and/or consultations with Supervisory Authorities that Customer is required to carry out under EU+ Data Protection Legislation; and (ii) making available to Customer information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and, not more than once per calendar year during the Term unless otherwise required by EU+ Data Protection Legislation, allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

7.24 Operational clarifications:

(a) When complying with its transparency obligations under Clause 8.3 of the EU SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, LogRhythm's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

(b) Where applicable, for the purposes of Clause 10(a) of Module Three of the EU SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for LogRhythm to notify any third party controller of any data subject request and that any such notification shall be the sole responsibility of Customer.

(c) To the extent legally permitted, Customer shall be fully responsible for any costs arising from LogRhythm's provision of any cooperation and assistance provided under Sections 7.21–7.23 above, and shall on demand reimburse LogRhythm any such costs incurred by LogRhythm.

(d) The audits described in: (i) Clauses 8.9(c) and 8.9(d) of the EU SCCs; and (ii) Clauses 5(f) and 12(2) of the UK SCCS, shall be subject to any relevant terms and conditions detailed in Sections 7.23(ii) and 7.24(c).

CHANGE IN CONDITIONS

7.25 If LogRhythm:

(e) determines that it is unable for any reason to comply with its obligations under this DPA and LogRhythm cannot cure this inability to comply; or

(f) becomes aware of any circumstance or change in the EU+ Data Protection Legislation, that is likely to have a substantial adverse effect on LogRhythm's ability to meet its obligations under this DPA;

LogRhythm shall promptly notify Customer thereof, in which case Customer will have the right to temporarily suspend the Processing until such time the Processing is

adjusted in such a manner that the non-compliance is remedied. To the extent such adjustment is not possible, Customer shall have the right to terminate the relevant part of the Processing by LogRhythm.

DELETION OR RETURN OF PERSONAL DATA

7.26 Deletion/Return. Upon termination or expiration of this Agreement, LogRhythm will:

(a) In accordance with the terms of the Agreement, delete or make available to Customer for retrieval all relevant Personal Data (including copies) in LogRhythm's possession;

(b) Except that if LogRhythm is required by applicable law from deleting/destroying the Personal Data, LogRhythm shall extend the protections of the Agreement and this DPA to such Personal Data and limit any Processing of such Personal Data to only those limited purposes that require retention, for so long as LogRhythm maintains the Personal Data.

7.27 Operational clarification relevant to SCCs. Certification of deletion of Personal Data as described in:

(a) Clause 12(1) of the UK SCCs; and

(b) Clauses 8.5 and 16(d) of the EU SCCs,

shall be provided only upon Customer's written request.

LIABILITY

7.28 The total aggregate liability of either party towards the other party, howsoever arising, under or in connection with the Agreement (including this DPA) and the SCCs (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the parties in the Agreement; **provided that**, nothing in this 7.28 will affect any person's liability to Data Subjects under the third party beneficiary provisions of the SCCs (if and as they apply) if and to the extent any such limitation(s) or exclusion(s) is prohibited by those SCCs and/or the EU+ Data Protection Legislation.

UK OFFICIAL

Framework Schedule 6

UK OFFICIAL

SCHEDULE 1

DETAILS OF THE PROCESSING

This Schedule includes certain details of the Processing of Personal Data, as required:

- by Article 28(3) GDPR; and
- to populate the Appendices of the SCCs in the manner described in those Appendices.

LOGRHYTHM DETAILS:

- **Name**: "LogRhythm" as defined in the pre-amble to the DPA.
- **Address**: 4780 Pearl E Cir, Boulder, CO 80304
- **Contact details**: privacyofficer@logrhythm.com
- **LogRhythm activities**: LogRhythm is a security intelligence company specialising in the provision of certain 'next generation' security information and event management or 'SIEM' offerings – including the provision of the Services to the Customer, and certain associated Processing of Personal Data on Customer's behalf, subject to and in accordance with the Agreement.
- **Role (controller/processor)**: Processor

CUSTOMER DETAILS:

- **Name**: "Customer" as defined in accordance with the DPA.
- **Address**: the Customer's address as shown in the Order entered into by and between the Customer and LogRhythm associated with the Agreement; or if no such Order has been agreed, the Customer's principal business trading address.
- **Contact details**: the Customer's contact details shown in the Order entered into by and between the Customer and LogRhythm associated with the Agreement; or if no such Order has been agreed, the Customer's contact details submitted by Customer and associated with Customer's account for the Services.
- **Customer activities**: Customer (whose particulars are set out in the execution block of the DPA) is a customer of the Services, and the entity on whose behalf Personal Data will be Processed in the context of LogRhythm's provision of those Services, subject to and in accordance with the Agreement and the DPA.
- **Role (controller/processor)**:
    - Controller – in respect of any Restricted Transfer, which involves Processing of Personal Data in respect of which Customer is a Controller in its own right; and
    - Processor – in respect of any Restricted Transfer, which involves Processing of Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including Authorized Affiliates).

DETAILS OF PROCESSING:

- **Categories of Data Subjects**: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:
    - Users on Customer's IT infrastructure that produce logs which are ingested into the LogRhythm platform.
- **Categories of Personal Data**: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data – the following types of 'personal data' comprised within Customer Data (as defined in the Agreement):
    - Personal identifiers common to log sources including First name, last name, job title, email address.
    - Indirect identifiers supplied by IT logs including IP address, MAC address, device ID and hostnames.
    - Inferable identifiers provided in logs, potentially including network access, browsing information or business system access.
- **Sensitive Categories of Data, and associated additional restrictions/safeguards**: none.
- **Nature of the Processing**: LogRhythm will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Customer in accordance with the DPA.
- **Purpose of the Processing**: to enable LogRhythm to provide, and Customer to receive, Services under and in accordance with the Agreement.
- **Duration of Processing / Retention Period**: Subject to Section 7.26 of the DPA, LogRhythm will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.
- **Transfers to (sub-)processors**: transfers to Sub-processors are as, and for the purposes, described from time-to-time in the Sub-processor List.

COMPETENT SUPERVISORY AUTHORITY

For the purposes of Part C of Annex I of the Appendix to the EU SCCs, the competent supervisory authority shall be determined as follows:

- Where the Customer is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which Customer is established.

- Where the Customer is ***not*** established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which Customer's EU representative relevant to the processing hereunder is based (from time-to-time).

- Where the Customer is ***not*** established in an EU Member State, Article 3(2) of the GDPR applies, but Customer has ***not*** appointed an EU representative under Article 27 of the GDPR, the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to privacyofficer@LogRhythm.com, which must be an EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

UK OFFICIAL

Framework Schedule 6

Framework Schedule 6

SCHEDULE 2

UK SCCs

Notes:

- The UK SCCs set out in this Schedule 2 are incorporated into and form an effective part of the DPA (if and where applicable in accordance with Section 7.15 of the DPA).
- Unless otherwise defined in this Schedule 2, capitalized terms used in this Schedule 2 have the meanings given to them in the DPA.

For the purposes of Article 46 of the UK GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection:

Customer, on its own behalf as a Controller, or as agent for applicable Controllers to the extent Customer is acting as a Processor (the '**data exporter**')

Address: as set out in or determined by Schedule 1 of the DPA.

Contact person's name, position and contact details: as set out in or determined by Schedule 1 of the DPA.

and

LogRhythm (the '**data importer'**)

Address: as set out in or determined by Schedule 1 of the DPA

Contact person's name, position and contact details: as set out in or determined by Schedule 1 of the DPA.

each a **party**; together **the parties**,

HAVE AGREED on the following Contractual Clauses (the '**Clauses**') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer''* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any

other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent,

the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

   (b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub- processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after termination

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

UK OFFICIAL

APPENDIX 1 TO UK SCCs

Data exporter

The data exporter is:

Name: Customer (as described in and determined by Schedule 1 of the DPA), on its own behalf as a Controller, or as agent for applicable Controllers to the extent Customer is acting as a Processor

Activities relevant to the data transferred under these Clauses: as set out in Schedule 1 of the DPA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Name: LogRhythm (as described in and determined by Schedule 1 of the DPA).

Activities relevant to the data transferred under these Clauses: as set out in Schedule 1 of the DPA.

Data subjects

As set out in Schedule 1 of the DPA.

Categories of data

As set out in Schedule 1 of the DPA.

Special categories of data (if appropriate)

As set out in Schedule 1 of the DPA.

Processing operations

As set out in or determined by Schedule 1 of the DPA.

APPENDIX 2 TO UK SCCs

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those established and maintained under Section 7.4 of the DPA and Schedule 4 (Security Measures) of the DPA.

SCHEDULE 3

EU SCCs

Notes:

- The EU SCCs set out in this Schedule 3 are incorporated into and form an effective part of the DPA (if and where applicable in accordance with Section 7.14 of the DPA).
- Unless otherwise defined in this Schedule 3, capitalized terms used in this Schedule 3 have the meanings given to them in the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

[**NOT USED**]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter

that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and

organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION [**NOT USED**]

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least the advance notice period determined by Section 7.9 of the DPA into which these Clauses are incorporated, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION [**NOT USED**]

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least the advance notice period determined by Section 7.9 of the DPA into which these Clauses are incorporated, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature

of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a)

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

For Module Three: The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Framework Schedule 6

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

DATA EXPORTER:

Name: Customer (as described in and determined by Schedule 1 of the DPA).

Address: as set out in or determined by Schedule 1 of the DPA.

Contact person's name, position and contact details: as set out in or determined by Schedule 1 of the DPA.

Activities relevant to the data transferred under these Clauses: as set out in Schedule 1 of the DPA.

Signature and date: these Clauses are hereby deemed to be entered into by Customer under and in accordance with Section 7.14 of the DPA with effect from the effective date of the DPA.

Role (controller/processor): as set out in or determined by Schedule 1 of the DPA.

DATA IMPORTER:

Name: LogRhythm (as described in and determined by Schedule 1 of the DPA)

Address: as set out in or determined by Schedule 1 of the DPA.

Contact person's name, position and contact details: as set out in or determined by Schedule 1 of the DPA.

Activities relevant to the data transferred under these Clauses: as set out in Schedule 1 of the DPA.

Signature and date: these Clauses are hereby deemed to be entered into by LogRhythm under and in accordance with Section 7.14 of the DPA with effect from the effective date of that DPA.

Role (controller/processor): as set out in or determined by Schedule 1 of the DPA.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred: as set out in Schedule 1 of the DPA.

Categories of personal data transferred: as set out in Schedule 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards: as set out in or determined by Schedule 1 of the DPA.

The frequency of the transfer: ongoing – as initiated by the Customer in and through its use, or use on its behalf, of the Services.

Nature of the processing: as set out in or determined by Schedule 1 of the DPA.

Purpose(s) of the data transfer and further processing: as set out in or determined by Schedule 1 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: as set out in or determined by Schedule 1 of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: as set out in or determined by Schedule 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

As set out in or determined by Schedule 1 of the DPA.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

General: Please refer to Schedule 4 (Security Measures).

[Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures:

- *Measures of pseudonymisation and encryption of personal data*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*
- *Measures for user identification and authorisation*
- *Measures for the protection of data during transmission*
- *Measures for the protection of data during storage*
- *Measures for ensuring physical security of locations at which personal data are processed*
- *Measures for ensuring events logging*
- *Measures for ensuring system configuration, including default configuration*
- *Measures for internal IT and IT security governance and management*

- *Measures for certification/assurance of processes and products*
- *Measures for ensuring data minimisation*
- *Measures for ensuring data quality*
- *Measures for ensuring limited data retention*
- *Measures for ensuring accountability*
- *Measures for allowing data portability and ensuring erasure]*

Sub-processors: When LogRhythm engages a Sub-processor under these Clauses, LogRhythm shall enter into a binding contractual arrangement with such Sub-processor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the DPA – including in respect of:

- applicable information security measures;
- notification of Security Incidents to LogRhythm;
- deletion of Personal Data as and where required; and
- engagement of further sub-processors.

Framework Schedule 6

SCHEDULE 4 – SECURITY MEASURES

LogRhythm will implement and maintain at least the following security measures set out in this Schedule 4 in respect of Personal Data Processed under this DPA:

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of LogRhythm's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to LogRhythm's organization, monitoring and maintaining compliance with LogRhythm's policies and procedures, and reporting the condition of its infor- mation security and compliance to internal senior management.

3. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:

   (a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly – which shall be encrypted using modern Transport Layer Security protocols; or

   (b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes) – which shall be encrypted using Advanced Encryption Standard (AES) 256-bit encryption.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job func- tions occur).

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that LogRhythm passwords that are assigned to its employees must:

   (a) be at least eight (8) characters in length;

   (b) not be stored in readable format on LogRhythm's computer systems;

   (c) be changed every ninety (90) days;

   (d) have defined complexity;

   (e) have a history threshold to prevent reuse of recent passwords; and

   (f) if newly-issued, be changed after first use.

6. Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to:

   (a) protect information assets from unauthorized physical access,

   (b) manage, monitor and log movement of persons into and out of LogRhythm facilities, and

   (c) guard against environmental hazards such as heat, fire and water damage.

7. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to LogRhythm's technology and information assets.

8. Incident / problem management procedures designed to allow LogRhythm to investigate, respond to, mitigate and notify of events related to LogRhythm's technology and information assets.

9. Network security controls that provide for the use of enterprise firewalls and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

10. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

11. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

LogRhythm may update or modify these Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services and/or relevant Personal Data.

UK OFFICIAL

[SCHEDULE 5] Authorized Sub-processors

Sub-processor	Function	Location
Amazon Web Services	Cloud Services Provider	EU (Customer may specify based on business need)
[●]	[●]	[●]
[●]	[●]	[●]]

15482 - RM6068 - UK Shared Business Services - Advanced Network Security Ltd - Customer v2