ATOS SUPPLIER TERMS FOR G-CLOUD 15

INTRODUCTION

1. The Atos Supplier Terms set out in this document (the "**Supplier Terms"**) form part of any call-off contract entered into between the Supplier and a Buyer under the G-Cloud 15 Framework Contract (the "**Framework Contract"**) and the applicable Order Form (together, the **Call-Off Contract**).

2. The Supplier Terms comprise:
   2.1 **the Supplier Standard Terms**; and
   2.2 **the Supplier Service Specific Terms**.

3. The **Supplier Standard Terms** consist of the Supplier Acceptable Use Policy, the Supplier Data Processing Agreement, and the Supplier-specific Shared Responsibility Model, each applying to a Call-Off Contract only where, and to the extent that, it is expressly incorporated by reference into that Call-Off Contract, unless otherwise agreed or stated in the Call-Off Contract.
   3.1 Supplier Acceptable Use Policy, which is attached to these Supplier Terms as Section 1 of Supplier Standard Terms. The Buyer's use of the Services may also be subject to one or more acceptable use policies of relevant Third-Party Providers, where applicable. ("**Acceptable Use Policy**" or "**AUP**").
   3.2 Supplier Data Processing Agreement, which is, attached to these Supplier Terms as Section 2 of Supplier Standard Terms, governs the processing of personal data in connection with the Services. The Buyer's use of the Services may also be subject to one or more data processing agreements of relevant Third-Party Providers (whether as a sub-processor or otherwise). ("**DPA**").
   3.3 Supplier-Specific Shared Responsibility Model, which is attached to these Supplier Terms as Section 3 of Supplier Standard Terms or referred to in the Service Description for the relevant services, describes the allocation of responsibilities between the parties in respect of the Services, unless otherwise agreed or stated in the applicable Order Form. The Buyer's use of the Services may also be subject to the shared responsibility model of any relevant Third-Party Provider, where applicable. **("Shared Responsibility Model").**
   3.4 Any of the above mentioned third-party AUPs, DPAs and Shared Responsibility Models policies shall apply and shall form part of the applicable Call-Off contract where they are been expressly set out in or referred to (by way of hyperlink or otherwise) in the relevant Order Form.

4 The **Supplier Service Specific Terms** consist of the Supplier service level agreement (SLA) for the Services; and the Supplier licence terms for the Services.
   4.1 The general Supplier Service Level Agreement ("**General SLA**") applicable to the Services is attached to these Supplier Terms as Section 1 of Supplier Service Specific Terms, in addition to the SLA referenced in the Service Definition for the relevant Services. The provision of the Services may also be subject to one or more service level agreements of relevant Third-Party Providers, where applicable. Any such third-party service level agreements shall apply where they are expressly set out in or referred to (by way of hyperlink or otherwise) in the relevant Order Form. The General SLA, the additional SLA in the Service Definition Documents, and any applicable third-party SLA shall collectively constitute the applicable SLA for the relevant Services **("Supplier Service Level Agreement" or "Supplier SLA**"); and
   4.2 The Supplier Licence Terms applicable to the Services are attached to these Supplier Terms as Section 2 of Supplier Service Specific Terms. The Buyer's use of the Services may also be subject to one or more licence terms of relevant Third-Party Providers, where applicable. Any such third-party licence terms shall apply only where they are expressly set out in or referred to (by way of hyperlink or otherwise) in the relevant Order Form. The Supplier Licence Terms and any applicable third-party licence terms shall collectively constitute the applicable licence terms for the relevant Services ("**Supplier Licence Terms**").
   4.3 The Supplier SLA and the Supplier Licence Terms shall form part of the applicable Call-Off Contract.

5. The Supplier Licence Terms have been split into separate parts to deal with the different types of Services that can be ordered by a Buyer.
   6.1 Where the Services ordered by a Buyer include or are solely Infrastructure-as-a-Service ("**IaaS**") and/or Platform-as-a-Service ("**PaaS**"), then Part A (Supplier Licence Terms – For PaaS or IaaS) of the Supplier Terms shall apply.
   6.2 Where the Services ordered by a Buyer include or are solely Software-as-a-Service ("**SaaS**"), Infrastructure Software ("**I-SaaS**"), or other online services (SaaS), Parts B (Supplier Licence Terms – For SaaS or I-SaaS), the Supplier Terms shall apply;
   6.3 Where the Services ordered by a Buyer include cloud-related IT planning, setup and migration, quality assurance and performance testing, security services, training, consultancy, application management, project management

and/or support services ("**Cloud Support Services**"), Parts C (Supplier Licence Terms - Cloud Support Services Terms) shall apply.

6.4 Parts D (Supplier Licence Terms – General) and Part E (Supplier Licence Terms- Definitions) shall always apply under the Supplier Licence Terms.

6.5 For the avoidance of doubt, where the Services ordered by a Buyer are a mixture of IaaS/PaaS, SaaS/IaaS and/or Cloud Support Services and SaaS, then the relevant Parts of the Supplier Licence Terms shall apply as relevant to the Service being provided.

7. Unless otherwise defined in these Supplier Terms, capitalised terms shall have the meanings given to them in the Call-Off Contract.

SUPPLIER STANDARD TERMS

SECTION 1 - ACCEPTABLE USE POLICY

A. This Acceptable Use Policy ("**Acceptable Use Policy**" or "**AUP**") sets out a non-exhaustive list of prohibited access to and/or use of the Buyer Account, the Buyer Content and the Service Elements. By accessing and/or using the Buyer Account, the Buyer Content and/or the Service Elements, the Buyer agrees to comply with (and to procure that its End Users comply with) the terms of this Acceptable Use Policy at all times.

B. The Buyer is responsible for breaches of this Acceptable Use Policy by it, its End Users and by any third party who accesses and/or uses the Buyer Account, the Buyer Content and/or the Service Elements (where such third party is acting on behalf of the Buyer and/or any End User or where such third party access and/or use is as a result of a Buyer and/or End User act, omission or default). Any breach of this Acceptable Use Policy is deemed to be a Material Breach of the Supplier Terms.

C. If a violation of this Acceptable Use Policy occurs or is reasonably suspected, the Supplier may suspend, restrict or terminate the Buyer's and/or any End User's access to and/or use of the Buyer Account, the Buyer Content and/or the Service Elements (or any part thereof) in accordance with the terms of the Call-Off Contract.

D. Unless otherwise defined herein, all capitalised terms used within this Acceptable Use Policy shall have the same meaning as ascribed to such terms in the Call-Off Contract or the Supplier Terms (as the case may be) and this Acceptable Use Policy shall be deemed by the Supplier and the Buyer to be subject to and form part of the Call-Off Contract.

1. ILLEGAL, HARMFUL OR OFFENSIVE USE OR CONTENT

1.1 The Buyer and its End Users shall not access and/or use or encourage, promote, facilitate or instruct others to access and/or use the Buyer Account, the Buyer Content or the Service Elements for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available Content (including any links to any Content) that is illegal, harmful, or offensive, or in each case which the Supplier in its reasonable opinion believes is so, including, but not limited to, the following:

1.2 Activities

1.2.1 any illegal activities, including offering, advertising, transmitting, disseminating, promoting or otherwise making available illegal sites, services, goods, schemes or promotions;

1.2.2 any activities that may be harmful to the Supplier's, any Supplier Party's or to any third-party systems, operations or reputation, including: (i) distributing any virus or worm or other harmful code other Malicious Software; (ii) hacking or perpetrating any security breach or penetration testing without the Supplier's prior written consent; (iii) unauthorized access to any device, computer, network or system; (iv) violating the privacy rights, publicity rights and/or Intellectual Property Rights of the Supplier, any Supplier Party or any third party (v) "mirroring" or "framing" of any part of the Service Elements or creating internet links to the Service Elements which include log-in information, user names, passwords, and/or secure cookies; (vi) introducing Content with the purpose of deliberately overloading the Supplier's, any Supplier Party's or any third-party system including denial-of-service activity or resource exhaustion; (vii) using the Service Elements (or any part thereof) in the operation of a service bureau or time sharing service or resale environment, unless expressly permitted; (viii) using Internet relay chat ("IRC"), including hosting of an IRC server, running IRC bots, use of a Supplier server as an IRC client or proxy, and use of IRC scripts or programs that interfere with service to other users on any server or network;

1.2.3 any activities that are abusive, deceptive, pornographic, obscene, defamatory, slanderous, offensive, threatening or otherwise inappropriate;

Content

1.2.4 any Content that constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts;

1.2.5 any Content that is excessively violent or that incites or threatens violence or is harassing or promotes hatred;

1.2.6 any Content that creates a risk to a person's or to public safety or health or compromises national security (including any information that would assist the construction of explosive, radioactive or other devices that could form a weapon) or interferes with an investigation by law enforcement;

1.2.7 any Content that violates the privacy rights, publicity rights and/or Intellectual Property Rights of the Supplier, any Supplier Party or any third party;

1.2.8 any Content that may damage, interfere with, intercept or expropriate any system, program or data, including exploits, malware or Trojan horses;

1.2.9 any Content that is obscene, abusive, malicious, fraudulent or otherwise objectionable or that exposes the Supplier or Supplier Parties to regulatory, reputational or operational risk; or

1.2.10 any Content that is otherwise illegal or solicits or promotes conduct that is illegal under any law.

2 SECURITY VIOLATIONS

2.1 The Buyer and its End Users shall not access and/or use, or encourage, promote, facilitate or instruct others to access and/or use the Service Elements, the Buyer Content or the Buyer Account in a manner that would compromise or harm the security or integrity of any information technology service or system (including any network, computer, device, communication system or software application), including by means of:

2.1.1 unless otherwise agreed, any API other than that made available or authorised by the Supplier;

2.1.2 unauthorised access and/or use, including attempting to probe, scan, or test the vulnerability of any information technology service or system or to breach any security or authentication measures used by any information technology service or system;

2.1.3 the monitoring of data or traffic without permission; or

2.1.4 fraud or other forms of misrepresentation.

3 NETWORK ABUSE

3.1 The Buyer and its End Users shall not make network connections or encourage, promote, facilitate or instruct others to make network connections to any users, hosts or networks without the prior written permission of such user, host or network, including where such connection is used for or is intended to be used for:

3.1.1 monitoring or crawling any information technology service or system which impairs or disrupts it from being monitored or crawled;

3.1.2 issuing excessive and unnecessary communications requests to a target which impede its response to genuine traffic or cause it to respond slowly, such as to become ineffective;

3.1.3 interfering with the proper functioning of an information technology service or system in any way, including by any attempt to overload the service or system;

3.1.4 operating network services like mail relays, recursive domain name servers or open proxies; or

3.1.5 circumventing usage limits, billing controls or technical safeguards.

4 MESSAGE ABUSE

4.1 The Buyer and its End Users shall not and shall not encourage, promote, facilitate, instruct or allow others to:

4.1.1 distribute, publish, send or issue (whether directly or indirectly) any unsolicited mass email, or other messages, solicitations, advertising, or promotions (e.g. “spam”) for any purpose, whether legal or illegal;

4.1.2 take any action that leads to a Spamhaus listing for any Supplier, Supplier Party or third-party IP address or in relation to the Buyer’s own IP addresses. If any action results in a Spamhaus listing, the Buyer shall cooperate with the Supplier, at its own expense, in clearing the IP address(es) from the Spamhaus RBL (and such assistance does not limit any other rights or remedies of the Supplier);

4.1.3 alter, obscure or otherwise tamper with mail headers or assume a sender’s identity without the sender’s prior written permission;

4.1.4 use an internet account or computer without the owner’s authorisation, including, but not limited to, internet scanning (tricking other people into releasing their passwords), password robbery, security hole scanning, and port scanning; or

4.1.5 collect replies to messages sent from the Supplier, any Supplier Party or any third party in breach of this Acceptable Use Policy or the policies and/or procedures of the Supplier, a Supplier Party or third party (as the case may be).

5 COMPLETE DEVELOPMENT ENVIRONMENT

5.1 Where a development, test or staging environment is provided, it must not be used in a live production or operational environment unless expressly authorised in writing.

6 OTHER

6.1 The Buyer and its End Users shall not access and/or use the Service Elements, the Buyer Account or the Buyer Content for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes, nor shall the Buyer or any End User provide information to third parties that could assist in such monitoring or benchmarking.

6.2 The Buyer and its End Users shall not use any shared system provided by the Supplier or a Supplier Party in a way that

unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the shared system, as may be set out in the relevant Services Description or the Order Form. Where this is not set out in the relevant Services Description or the Order Form, what constitutes an interference with the normal operation of a shared system or what constitutes consumption of a disproportionate share of the resources of the shared system shall be determined in accordance with market practice.

6.3 The Buyer agrees that the Supplier may quarantine or delete any Buyer Content (or any part thereof) stored on a shared system if the Buyer Content (or any part thereof) is infected with Malicious Software, a virus, or is otherwise corrupted, and has the potential to infect or corrupt the shared system or other Content that is stored on the shared system.

7 ENFORCEMENT

7.1 The Supplier reserves the right (but is not obliged), to investigate any breach of this Acceptable Use Policy or any inappropriate access and/or use of the Service Elements, the Buyer Content and/or the Buyer Account at any time, and as a consequence of which the Supplier may:

7.1.1 block or disable the Buyer's or any End User's access and/or use of the Service Elements, the Buyer Account and/or the Buyer Content; or

7.1.2 modify any Content used by the Buyer or any End User that is in breach of this Acceptable Use Policy or the Call-Off Contract;

7.1.3 suspend or terminate the provision of the Service Elements or the Buyer Account in accordance with the terms of the Call-Off Contract;

7.1.4 investigate and/or report any illegal, harmful or offensive Content, activity, access and/or use to the appropriate authorities or third parties; or

7.1.5 co-operate with the appropriate authorities and/or third parties in relation to any investigation and provide them with such information as they may require for the purposes of their investigations without notifying the Buyer or any End User.

8 REPORTING

8.1 If the Buyer and/or any End User become aware of any actual or likely breach of this Acceptable Use Policy the Buyer shall, and the Buyer shall procure that any End User shall, notify the Supplier immediately and provide the Supplier with all information relating to any such actual or likely breach and assist the Supplier, as reasonably requested, to stop or remedy such breach.

8.2 To report any breach of this Acceptable Use Policy, please contact: gcloud@atos.net

9. DISCLAIMER

9.1 The Supplier is under no duty and does not by this Acceptable Use Policy undertake a duty to monitor or police the Buyer's and/or any End User's activities or Content. The Supplier has no obligation to any third party who has not entered into an agreement with the Supplier for the Service Elements other than as required by law.

SECTION 2 - SUPPLIER DATA PROCESSING AGREEMENT

Atos Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of any Call-Off Contract under the G-Cloud 15 Framework Contract **(the "Agreement")** between the Buyer and Atos IT Services UK Ltd, a company incorporated under the laws of England with its registered office at Second Floor, Mid City Place, 71 High Holborn, London, WC1V 6EA **("Supplier").**
The Buyer and the Supplier shall each be referred to as a **"Party"** and together as the **"Parties."**

The Supplier shall maintain appropriate and adequate administrative, physical and technical safeguards to protect the security, confidentiality and integrity of the Buyer's data, as required under the Framework Contract and all Call-Off Contracts. These safeguards shall include, but are not limited to, measures that prevent access, use, modification or disclosure of the Buyer's data by third parties or Supplier personnel except:
(a) as necessary to provide the Services or to prevent or address service or technical issues;
(b) as required by law, in accordance with this DPA; or
(c) as expressly authorised in writing by the Buyer.

To the extent that the Supplier processes any Personal Data (as defined in this DPA and the Framework Contract) on behalf of the Buyer in connection with the Services, the terms of this DPA are hereby incorporated by reference, and the Parties agree to comply with them. For the purposes of the Standard Contractual Clauses (where applicable), the Buyer is the data controller and data exporter.

This DPA sets out the Parties' respective obligations regarding the processing of Personal Data by the Supplier on behalf of the Buyer for the purpose of performing the Services under the Agreement. Both Parties shall act in accordance with applicable data protection principles and all relevant legal and contractual requirements.
.

1. Definitions

1.1 Capitalised terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified or supplemented below, the definitions of the Agreement shall remain in full force and effect. For the purpose of interpreting this DPA, the following terms shall have the meanings set out below:

Verb	meaning
"**Applicable Laws**"	means all current and future laws and regulations (as may be amended or updated from time to time) applicable to the Processing of Personal Data under the Agreement, including the Data Protection Act 2018 and the UK GDPR and any other applicable laws of any other country, province, state or jurisdiction to which the Processing of the Personal Data is subject.
"**Data Controller**" (or Controller)	shall have the meaning given in the Applicable Laws.
"**Data Processor**" (or Processor)	shall have the meaning given in the Applicable Laws.
"**Processing**" (or any cognate terms)	shall have the meaning given in the Applicable Laws.
"**Personal Data**"	shall have the meaning given in the Applicable Laws.
"**Personal Data Breach**"	shall have the meaning given in the Applicable Laws.
"**Sub-Processor**"	shall have the meaning given in the Applicable Laws.
"**Third Country**"	means any country outside of the European Economic Area ("**EEA**") plus any jurisdictions defined as a Third Country by the European Data Protection Board ("**EDPB**").

2. Roles and Obligations of the Parties

2.1 For the purpose of Processing Personal Data, both Parties acknowledge and recognise being bound by the duties and obligations of the Applicable Laws and the following subsequent conditions.

2.2. The purpose of this DPA is to frame the Processing of Personal Data in connection with the terms of the Agreement, regardless of the country of origin, place of Processing, location of Data Subjects, or any other factor.

2.3. The Parties expressly agree that (i) Buyer is the Data Controller for the Personal Data Processed for the purpose of the provision of the Services under the Agreement; and (ii) Supplier is the Data Processor in the event it Processes any Personal Data on behalf of and under the written instructions of Buyer when performing the Services.

3. Guarantees regarding Buyer's Processing

3.1. Buyer, as Data Controller, guarantees that any Personal Data provided to Supplier for processing for the purposes of the Agreement (hereinafter "Buyer Personal Data") is processed in accordance with Applicable Laws, including but not limited to its own obligations to the legitimacy of the processing, the categories of data processed, data subjects' rights (including information), the definition and implementation of adequate retention periods, the completion of relevant formalities, if any as well as any verifications and assurances regarding the adequacy of the guarantees provided by Supplier regarding the Processing and protection of Buyer Personal Data. In this respect, Buyer guarantees that it has taken all necessary steps to ensure that its own obligations are complied with under its applicable legislation.

4. Exchange of Business Data and Communication Between the Parties

4.1. In the context of the performance of the Agreement, the Parties may be required, for the purpose of communication, to exchange the following information:

4.1.1. personal information: first name, last name;

4.1.2. communications data: telephone, email, postal mail; and/or

4.1.3. other: Personal Data to which one Party provides access to the other for the purpose of communication between the Parties.

4.2. Both Parties undertake that each Party shall act as an independent Data Controller in order to process the above-mentioned Personal Data for their own means and purposes. Therefore, the Parties shall comply with the obligations of a Data Controller, as required by the Applicable Laws, in order to protect and secure the aforementioned Personal Data.

5. Buyer's Processing Instructions

5.1. As Data Controller, Buyer shall provide Supplier with written and lawful documented instructions regarding the Processing of Personal Data. The Parties agree that Buyer's instructions are a condition for Supplier to assist Buyer with complying with its obligations under Applicable Laws.

5.2. The Parties agree that Buyer's initial instructions for the Processing of Personal Data are set out in this DPA, including (a) the Description of Processing of Personal Data (Appendix 1) and (b) Technical and Organisational Measures (Appendix 2). Buyer shall notify Supplier in written form at least thirty (30) days before the desired date of implementation to evaluate Buyer's proposed additional instructions and assess the feasibility of the implementation timeframe.

5.3. In the event Buyer requests the implementation of modifications or additions to its instructions, it is expressly agreed between the Parties that it may have a direct impact on the delivery of the Services, which may require a review and modification of the terms of the Agreement, including, notably, the scope of the Services and cost of implementation. In such a case, the Parties shall use the change control procedures set forth in the relevant Clause of the Agreement.

6. Supplier's Obligations

6.1. Supplier shall process Personal Data on behalf of Buyer exclusively and only in accordance with the instructions received from Buyer as documented in Appendix 1 to this DPA, and additional instructions agreed by the Parties in Appendix 2.

6.2. If Supplier becomes aware that the instruction(s) it receives from Buyer constitute or may constitute an infringement of Applicable Laws, it shall immediately inform Buyer in any written form of such actual or potential infringement.

6.3. Supplier shall comply with any new, lawful, or revised instructions provided by Buyer, subject to Clause 6.2 of this DPA. In the event that Buyer's instructions are or may be in contradiction with Applicable Laws, Supplier is entitled to stop Processing, or the part of the Processing that is infringing the Applicable Law, and notify Buyer of such in order to obtain new, revised and lawful instructions.

6.4. 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, Supplier shall implement appropriate technical and organisational measures to ensure that Buyer Personal Data are processed as per applicable legal data protection requirements as set forth in the Appendices of this DPA.

6.5. Supplier confirms that its personnel in charge of Processing Personal Data in the context of the Agreement are bound by an appropriate obligation of confidentiality regarding the Processing of Personal Data. Supplier shall also ensure that its personnel in charge of Processing Personal Data in the context of the Agreement participate in mandatory training or e-learning regarding Privacy and Personal Data Protection.

7. Records of Processing Activities

7.1. Supplier shall maintain a record of categories of Processing activities carried out on behalf of Buyer regarding the Services provided under the Agreement, if required under Applicable Laws. Upon request from Buyer or from any competent supervisory authority (as may be required under Applicable Laws), Supplier shall provide a copy of such records of Processing activities without undue delay and, in any case, within fifteen (15) business days of such request, or within the timeframe defined by Applicable Laws.

8. Data Subject Rights

8.1. Whilst Buyer is responsible for determining the manner in which it responds to Data Subjects' requests to exercise their rights under Applicable Laws, Supplier shall, in accordance with Applicable Laws and taking into account the nature of the Processing, assist Buyer by appropriate processes to support Buyer in the fulfilment of the obligation to respond to Data Subjects' requests, including notably:

8.1.1. promptly notify Buyer if any Personal Data recipient receives a request that should have been directed to Buyer from a Data Subject under any Applicable Law with respect to Personal Data;

8.1.2. ensure that the Supplier Personal Data recipient does not respond to that request, except on the documented instructions of Buyer, where Buyer and Supplier have agreed that Supplier shall undertake that role, or as required by Applicable Laws to which the Supplier Personal Data recipient is subject, in which case Supplier shall, to the extent permitted by Applicable Laws, inform Buyer of that legal requirement before the Supplier Personal Data recipient responds to the request; and

8.1.3. comply with any documented instructions from Buyer regarding response to a request to exercise rights of the Data Subjects under Applicable Laws.

8.2. In relation to this Clause 8, the Parties shall communicate Personal Data in a structured, commonly used and machine-readable format.

9. Interactions with Supervisory Authorities

9.1. Upon Buyer's request, Supplier shall assist Buyer with complying with its obligations towards any competent data protection authority where required, including:

9.1.1. providing information relating to a Processing where it is required to support a request for approval or authorisation of a Processing;

9.1.2. providing information relating to a Processing in order to address any requests for information, controls or investigations; and/or

9.1.3. providing information in case of a Personal Data Breach as set out below in Clause 14 of this DPA.

10. Security of Processing

10.1. Taking into account the state of the art, 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, Supplier shall, in accordance with Applicable Laws, assist Buyer to comply with its obligation to define and implement adequate technical and organisational measures to ensure the security and confidentiality of the Personal Data Processed under this DPA.

11. Data Protection Impact Assessments

11.1. Supplier shall provide Buyer with information that is relevant regarding the processing of Personal Data performed by Supplier on behalf of Buyer, in order to enable Buyer to complete necessary documents (such as a data protection impact assessment).

12. Subprocessing

12.1. Buyer hereby expressly confirms and acknowledges that it has given its written consent to Supplier in order to transfer Personal Data to its third-party Sub-Processors for Personal Data Processing operations that are necessary to comply with its obligations under the Agreement. Supplier shall implement or rely on appropriate documentation (i.e., contracts, binding corporate rules, standard contractual clauses, codes of conduct, etc.) and technical additional safeguards (i.e., such as encryption and pseudonymised data, data non decryptable by national security agencies) to ensure that the Sub-Processor implements a level of protection for Buyer Personal Data similar to the provisions set out under this DPA.

12.2. If such transfer includes a transfer of Buyer Personal Data to a Third Country, the provisions set out in Clause 13 below of this DPA shall apply.

12.3. Buyer hereby expressly accepts the list of Sub-Processors in Appendix 1.

12.4. Supplier shall inform Buyer in writing of any intended changes to that list through the addition or replacement of Sub-Processors at least 30 days in advance of onboarding such a Sub-Processor.

13. Transfers of Buyer Personal Data to Third Countries

13.1. Supplier and its affiliates are bound by the Binding Corporate Rules of the Supplier Group ("**BCR**"), as approved by authorised agencies and set forth at: https://Supplier.net/en/Supplier-binding-corporate-rules. Buyer acknowledges that, in the event that Supplier transfers Buyer Personal Data to any Supplier affiliate located in a Third Country, the Supplier Group BCR (https://Supplier.net/content/bcr/eu/Supplier-binding-corporate-rules.pdf) and the Supplier UK BCR as Processor (https://Supplier.net/content/bcr/uk-p/Supplier-uk-bcr-as-a-processor.pdf) constitute a sufficient safeguard to establish that such entities provide an adequate level of protection to Personal Data as required under Applicable Law.

13.2. Supplier shall ensure that its Sub-Processors authorised by Buyer to Process Buyer Personal Data provide an adequate level of protection for such Buyer Personal Data. For that purpose, Supplier shall: (i) ensure that any Sub-Processor authorised to Process Buyer Personal Data in a Third Country shall comply with the obligations set out in appropriate

standard contractual clauses for the transfer of Personal Data as set forth by the European Commission (or any competent authority) (in particular the European Commission's standard contractual clauses pursuant to Regulation (EU) 2016/679); or (ii) implement alternative means to the Standard Contractual Clauses, in order to ensure an adequate level of protection of Buyer Personal Data, if acknowledged as appropriate means by the competent European or local authorities.

14. Security and Confidentiality Measures

14.1. Buyer acknowledges that: (i) the technical and organisational security measures defined and applied by Supplier are based on the instructions and information it has received from Buyer, which are used to assess and evaluate, with Buyer, the risks associated with the Processing of Buyer Personal Data; and (ii) it has reviewed the technical and organisational security measures set forth in Appendix 2 (Information Security Requirements) and deems them adequate, taking into consideration the risks of the Processing, and the defined purpose of the Processing.

14.2. Buyer agrees that, in the event that it modifies its Processing instructions in accordance with the provisions of Clause 5 of this DPA, the technical and organisational security measures initially defined and implemented may no longer be adequate to the risks of the Processing and the defined purposes of the Processing. In such a case, Buyer agrees that such technical and organisational security measures may need to be amended and that such changes may have an impact on the delivery of the Services and the terms of the Agreement, including, notably, the financial provisions.

14.3. Buyer shall inform Supplier in respect of any particular threats or vulnerabilities that it becomes aware of. Additionally, Buyer acknowledges that significant security threats and vulnerabilities may, from time to time, occur and be identified by Supplier. Where such threats and vulnerabilities result from or are connected to Buyer's technical or operational decisions (e.g., initial security measures decided, systems implemented, etc.), Supplier shall, without undue delay, notify Buyer of said threat or vulnerability when it becomes aware of such threat or vulnerability. Supplier shall, where possible, recommend a course of action or remediation to suppress, mitigate or limit the impact of the threat or vulnerability, and the Parties shall agree to any such changes under the change control procedures set forth in the relevant clause of the Agreement. Buyer shall bear any costs related to Supplier's efforts to mitigate threats or vulnerabilities resulting from Buyer's actions.

15. Personal Data Breaches

15.1. In the event of a Personal Data Breach arising during the performance of the Services by Supplier, Supplier shall, without undue delay, after having become aware, notify Buyer about the Personal Data Breach, and provide the following: (i) where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of data records concerned; (ii) where possible, the name and contact details of the relevant contact point where more information can be obtained; and (iii) where possible, describe the likely consequences of the Personal Data Breach.

15.2. In case of a Personal Data Breach, Supplier shall:

15.2.1. take, in coordination with Buyer, all relevant further actions as may be necessary to limit the effects of the Personal Data Breach;

15.2.2. assist Buyer in order to define and implement all actions as may be required under Applicable Laws (including any notifications to competent data protection authorities);

15.2.3. maintain a record of information relating to the Personal Data Breach, including, where possible, the results of its own investigations and/or authorities' investigations; and

15.2.4. cooperate with Buyer and take necessary measures to prevent such a Personal Data Breach from occurring again.

15.3. In the event of such a Personal Data Breach, both Parties shall treat any information regarding the Personal Data Breach with the highest degree of confidentiality and actively cooperate on any public communication and/or official notification to competent authorities.

16. Legal Requests for Access to Buyer Personal Data

16.1. In the event Supplier is requested or required under Applicable Laws or regulatory obligations to conduct certain Processing operations (including but not limited to disclosure to public authorities) relating to Buyer Personal Data, in a Third Country that does not provide a level of protection to personal data that is essentially equivalent to that provided for in the EEA and/or the UK, and in the context of mass surveillance or surveillance measures Supplier hereby expressly undertakes to: (i) inform Buyer of such request or requirement as soon as possible (subject to compliance with legal provisions which may prevent it from informing Buyer) in order to obtain Buyer's express and written consent to such Processing operations; (ii) oppose, where possible, such request or requirement (including, notably, by advising that Supplier does not own nor control the data it Processes on behalf of Buyer); or (iii) assist Buyer, if possible and at Buyer's cost, in any action undertaken (if Buyer so decides) to oppose such Processing operations.

17. Audit Rights

17.1. Buyer may, once a year, and subject to prior written notice of two (2) months where possible and otherwise a reasonable notice period of at least four (4) weeks, conduct, or have an independent duly appointed third party established on the market for its auditing functions, an audit of Supplier's Processing facilities in order to ensure Supplier's compliance with

the obligations set forth in this DPA. Any third party conducting an audit on Buyer's behalf shall be bound by a strict obligation of confidentiality and shall not be a Supplier's competitor. Such audit shall not hinder or disrupt Supplier's operations or business activities and shall only relate to that part of the relevant information technology infrastructure which processes Buyer's Personal Data.

17.2. The party conducting the data protection audit shall bear its own costs for audits. Such audits will incur time and material fees for the party conducting the audit, unless otherwise agreed between the Parties in the Agreement.

18. No Selling of Personal Data

18.1. Supplier acknowledges and confirms that it does not receive any Personal Data as consideration for any Services or other items that Supplier provides to Buyer. Buyer retains all rights and interests in its Personal Data. Supplier agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Supplier to qualify as selling Personal Data under Applicable Laws.

Appendix 1
GENERAL DESCRIPTION OF THE PROCESSING OF PERSONAL DATA CONDUCTED BY SUPPLIER

Contact information

Supplier affiliates	Supplier entity signing the Agreement ,		
Supplier 's DPO	Supplier Business Owner	Buyer's DPO	Buyer's Project Manager
Name: Mail: Dpo-global@atos.com Tel:	Name: Mail: Tel:	Name: Mail: Tel:	Name: Mail: Tel:

Service description

Please describe in few words the services or products provided by Supplier to Buyer	Please, specify: Example: project management software on demand, in a cloud computing environment. SaaS

Processing activities

Purpose of the Processing	Please describe the operation or set of operations which is performed on personal data Potential wording: Supplier as Data Processor will Process Personal Data as required to provide the Services described before and in accordance with the Agreement and this DPA. Example: Supplier will process personal data of users of the software to provide the services. Identification data to manage access…
Categories of Processing activities* (see definition list below)	Collection ☐ Consultation ☐ Storage ☐ Media Handling (e.g. shipping of tapes or optical media ☐ Organisation ☐ Disclosure ☐ Structuring ☐ Making Available ☐ Recording ☐ Alignment/Combination/Matching ☐ Adaptation ☐ Restriction of use or access ☐ Retrieval ☐ Erasure or destruction ☐ Remote Access ☐ Use ☐ Profiling ☐ Big Data Analytics Other (please, specify): _____
Location of the Data Subjects	European Union ☐ Non-European Union ☐ Please specify (non-EU): _____
Categories of Personal Data processed	Identification Data ☐ Connection Data ☐ Personal life ☐ Location Data ☐ Professional life ☐ Account profile ☐ Other (please, specify): _____

Categories of sensitive Personal Data processed	No sensitive Personal Data			☐
	Social Security Number or National Identification Number	☐	Trade-Union Affiliation	☐
	Biometric Data	☐	Health Information	☐
	Genetic Data	☐	Sexual Preferences	☐
	Banking and financial data	☐	Criminal offences and sanctions	☐
	Racial or ethnic data	☐	Other	☐
	Philosophical, Political or Religious Beliefs	☐	Telephone intercepts	☐
Categories of Data Subjects	Employees of the Buyer	☐	End-Users	☐
	Buyers of the Buyer	☐	Members	☐
	Supplier s	☐	Visitors	☐
	Other (please, specify): _____ _____ _____			
Term of retention/deletion of Personal Data	Please, specify: Potential wording if no term defined: Supplier as Data Processor will Process Personal Data for the duration of the Agreement and in accordance with this DPA and additional instructions provided by the Buyer. _____			

Supplier 's Data Protection practices

Supplier 's guarantees regarding the Processing of Personal Data **(please, attach the file or give the reference to find it)**	Data Protection/Privacy Policy/Binding Corporate Rules Reference: Supplier Binding Corporate Rules	☒
	Information Security Policy Reference: Supplier Information Security Policy	☒
	Policy regarding encryption of Personal Data Reference: Supplier Encryption Policy	☒
	Data access management and control rules Reference: Supplier Access Management Policy	☒
	Security standard certifications (e.g. ISO 27001) Supplier is certificated according to: • DIN EN ISO 9001: 2015 (Quality Management); • ISO / IEC 27001: 2013 (Information Security Management); • ISO / IEC 20000-1: 2011 (IT Service Management); • ISO / IEC 14001:2015 (Environmental Management)	☒

	Reference: provide certification with link if requested by Buyer	
	Data Subject's exercise rights process: Reference: Exercise your rights regarding your Personal Data - Supplier	☒
	Regular training of employees on Data Protection: Supplier has developed a Global Training Program which aims at providing general training to all Employees and specific training to Employees who have permanent or regular access to Personal Data. For more information refer to Supplier BCR	☒

Location of Supplier Processing activities (Supplier 's affiliates)

Name	Address	Country	Service Description
Affiliate 1			
Affiliate 2			
Affiliate 3			

Does Supplier use one or several external Sub-Processors?

YES ☐

NO ☐

List of Supplier external Sub-Processors subcontractors involved in the project

If yes, provide the information below of Supplier external subcontractors

Name	Address	Country	Service Description
Sub-Processor 1			
Sub-Processor 2			
Sub-Processor 3			

Safeguards implemented if Supplier 's affiliates or subcontractors are located outside the EU or if Personal Data is available from outside the EU

Supplier shall specify which measure it uses to frame the transfer of personal data to its subcontractors

Country recognised as providing an adequate level of protection by the EU Commission	☐
European Commission's Standard Contractual Clauses	☐
Specific (ad-hoc) data transfer agreement, requiring a high level of protection, duly validated by competent authorities	☐
Supplier 's validated Binding Corporate Rules	☒
Supplier 's adhesion to a validated code of conduct	☐

Please, specify:

_____

_____

The frequency of the transfer

One-off ☐

Continuous basis ☐

*** CATEGORIES OF PROCESSING ACTIVITIES**

Term	Definition
Adaptation	Providing services that transform existing data into a form more suitable for a particular purpose, for instance, by removing data that is not required for that purpose or by making it accessible via a different means.
Alignment / Combination / Matching	Providing services that process two or more Buyer data sets in order to either (a) validate or update one or more of them, or (b) create a further data set.
Big Data Analytics	Providing the means for analysing big data (big data is a massive amount of data sets that cannot be stored, processed, or analysed using traditional tools). Big Data Analytics allows the accumulation and/or interrogation of large data sets for the purpose of deriving novel insights or new data sets. For example, a process used to extract meaningful insights, such as hidden patterns, unknown correlations, market trends, and Buyer preferences.
Collection	Providing services that can directly obtain data, such as: providing a website that receives applications, processing written data, or contacting individuals to obtain data.
Consultation	Providing services that require reference to existing Buyer data sets in order to answer queries on behalf of the Buyer.
Disclosure	Providing services that copy or transmit Buyer data to an authorised third party for its own use (for example, a tax authority or a regulator).
Erasure or destruction	Providing services that permanently delete data so that it can never be recovered, either by securely wiping/overwriting it or by physically destroying the media on which it is stored.
Making available	Providing services that facilitate access to personal data, such as an internet or intranet service that provides user access to permitted data.
Media handling	Providing services that organise, store or transport media that contain Buyer's data.
Organisation	Providing services that improve data quality or accessibility, for example, by bringing data together in one place or removing duplication.
Profiling of individuals	Providing services that analyse personal data from one or more sources, leading to the evaluation of certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. In other words, it identifies characteristics of identifiable individuals and/or makes decisions, such as marketing decisions, that may subsequently have an impact on particular individuals (e.g. types of marketing they are sent or types of services they are offered).
Recording	Providing services that result in the storage of audio or video recordings, or creating data based on manual or automated observation to reproduce a scene. (e.g. electronic recording of voice or taking exact notes of a conversation)
Remote access	Providing the ability for an authorised person to access a computer or a network from a geographical distance through a network connection. It enables users to connect to the systems they need when they are physically far away.
Restriction of use or access	Providing services that allow specific data to be quarantined, for example, to meet legal obligations to restrict processing or to maintain evidential integrity of data for legal/regulatory purposes.
Retrieval	Providing services that process requests for finding personal data in, for example, archives or databases. Retrieval is the operation of accessing data, either from memory or from a storage device.
Use	"Use" is non-specific and covers a multitude of other processing categories as listed here. Please only refer back to this term if the processing comprises all other categories except profiling, combination and Big Data Analytics. Data in use is data that is currently being updated, processed, erased, accessed or read by a system. This type of data is not being passively stored, but is instead actively moving through parts of an IT infrastructure
Storage	Providing services that offer the means for storing (i.e. kept for actual or possible further use) Buyer data, such as cloud storage, backup or archiving.
Structuring	Providing services that help to arrange data in a way that makes information more accessible and easier to use for its intended purpose.

Appendix 2

INFORMATION SECURITY REQUIREMENTS

[The YES/NO responses are to *be provided by the Buyer and reviewed by Supplier Information Security.*]

TECHNICAL AND ORGANISATIONAL MEASURES
Technical and organisational measures are implemented according to the Global Data Protection Statement

Confidentiality

Physical Access Control The goal of physical access control is to deny unauthorised persons access to those data Processing systems that process or use Personal Data.	**YES/NO**
Supplier implements controls designed to stop unauthorised individuals to access to data Processing systems	
Supplier uses a partitioning of Data Centre rooms	
Supplier uses a video surveillance and intrusion detection systems in order to monitor access to data Processing systems	
Supplier has policies ensuring physical access control	
Logical Access Control The goal of logical access control is to prevent unauthorised persons from using data Processing systems that process and use Personal Data.	**YES/NO**
Supplier ensures that data Processing systems are accessed by means of authorisation and authentication in all systems	
Supplier assigns passwords to authorised persons	
Supplier assigns a company ID to authorised persons	
Supplier ensures that role-based rights are tied to access ID	
Supplier uses encryption of data storage devices while in transit	
Supplier ensures use of firewalls and antivirus software including regular security updates and patches	
Supplier has policies ensuring logical access control	
Application Access Control Application access control measures prevent unauthorised Processing and activities (e.g. unauthorised reading, copying, modification or removal) in data Processing systems by persons without the required level of authorisation.	**YES/NO**
Supplier ensures the system-wide authentication of all users and data terminals including access regulations and user authorisations	
Supplier implements a role-based authorisation concept	
Supplier ensures that access authorisation is always based on the principle of restrictive allocation of rights	
Supplier implements a program-related authorisation concept	
Supplier ensures that shared systems have Buyer separation/separate data pool	
Supplier has a clear desk policy is in place	
Supplier ensures that data storage devices in all mobile systems are encrypted while in transit	
Supplier uses the firewalls and antivirus software including regular security updates and patches	
Supplier carries out a regular review of all existing privileged accounts	
Separation Control The goal of separation control is to ensure that data collected for different purposes can be processed separately.	**YES/NO**
To the extent that there are no dedicated systems in use for exactly one Buyer, Supplier ensures that the employed systems are multi-tenant capable	
Development and quality assurance systems are completely separate from productive systems in order to ensure productive operation	
Supplier ensures that Buyer systems are only accessed by authorised persons from a secured administration network.	

Pseudonymisation The objective of the pseudonymisation regulation and control is that the Processing of Personal Data is carried out in such a way that the data can no longer be attributed to a specific Data Subject without additional information, provided that this additional information is kept separately and fall under the corresponding technical and organisational measures.	**YES/NO**
Supplier uses anonymised identifiers, which can only be resolved using a separate database	
Supplier uses server identifiers, which conceal conclusions on the function	
System hardening requirements include a strict prohibition on login banners with information about the type and version of the software used on the systems operated by Supplier	
Encryption measures The aim of the measures for the encryption of Personal Data is to protect the contents of databases from unauthorised access and alteration.	**YES/NO**
Supplier can ensure encryption of Personal Data following the given instruction from the controller	
Supplier uses point-to-point or end-to-end SSL-encrypted data transfer between systems	
Supplier ensures application-driven encryption of the data before transfer to databases	
Supplier ensures encryption of DB backups	
Supplier implements e-mail encryption	
Schrems II Security measures for personal data subject to EU GDPR The aim of the measures for the encryption of Personal Data is to protect the contents of databases from unauthorised access and alteration in countries which do not ensure an adequate level of protection regarding mass surveillance laws and surveillance measures.	**YES/NO**
Supplier ensures that the level of encryption and/or pseudonymisation is adequate compared to the risk level in the country of importation as per the assessment conducted before the transfer.	
Supplier ensures after encryption that the cryptographic keys remain either in the country of exportation, the European Union or in a third country recognised as providing a level of protection essentially equivalent to that guaranteed in the EU regarding mass surveillance laws and surveillance measures.	
Supplier ensures in case of transfers of personal data to third countries mentioned above, the importer must not have access to the personal data unencrypted.	
Supplier ensures that subject to request from Supplier it will provide documented proof that cryptographic keys are located as per Supplier ' requirements.	

Integrity

Transmission control The goal of transmission control is to ensure that Personal Data cannot be read, copied, modified, altered or removed while being transmitted, transported or saved to a data storage medium and that it can be checked and asserted where the transmission of Personal Data through transmission systems is intended	**YES/NO**
Supplier supports standard secure transmission types such as network-based encryption (server to server or server to Buyer and/or to suppliers) and encrypted connection tunnelling	
Supplier uses SSL certificate for websites (https://) to transfer data within forms	
Supplier has policy for mobile devices	
Supplier implements disposal of data storage devices in a manner compatible with data protection regulations	
Supplier has clear desk policy in place	
Supplier uses encryption of data storage media while in transit (including notebook hard drives)	
Input Control Measures that are suited for facilitating the belated checking and asserting if Personal Data has been entered into, changed within or deleted from data Processing systems and if so by whom	**YES/NO**
Supplier has implemented access regulations and user authorisations that enable the identification of all users and data terminals in the system	
All monitoring and logging measures are adapted to the state of the art and the criticality of the data to be protected and carried out in the associated economic framework	

Availability and resilience

Availability control The goal of availability control is to ensure that Personal Data is protected from accidental destruction, damage or loss.	**YES/NO**
Supplier ensures that Personal Data is stored at a minimum in systems which are protected against hardware-related data loss	
Supplier ensures that Personal Data is stored in secure and redundant systems up to a spatially separate area, in order to ensure a short recovery time and a high overall availability	
Supplier implements storage systems, in combination with appropriate software components, which are equipped with a technology that enables defined data from certain points of time to be recovered	
Supplier carries out the data backups on a regular basis according to existing service agreements	
Supplier ensures that the systems are powered without interruption	
Resilience / rapid recovery This measure ensures that Personal Data can be quickly recovered in the event of a physical or technical incident through an emergency management plan and regular recovery testing (at minimum annually	**YES/NO**
Supplier ensures that emergency planning / crisis planning in connection with emergency and restart plans for the data centers is available	
Emergency plans are subject to a regular and continuous audit and improvement process	

Other measures

Privacy by Design and Privacy by Default	**YES/NO**
Supplier ensures that Data Protection is taken into account at the earliest possible date by data protection-friendly presets in order to prevent unlawful Processing or the misuse of data.	
Supplier minimises the amount of Personal Data and ensures limitation of use	
Supplier pseudonymises or encrypts data as early as possible	
Supplier creates transparency with regard to procedures and Processing of data	
Supplier anonymises data as early as possible	
Supplier minimises access to data	
Supplier presets existing configuration options to the most privacy-friendly values	
Supplier documents the assessment of the risks to the persons concerned.	

SECTION 3 SHARED RESPONSIBILITY MODEL

SUPPLIER RESPONSIBILITIES

- Security Monitoring & Incident Operations: Deploy and manage security monitoring tools (SIEM/SOAR platforms, threat intelligence feeds). Provide 24×7 surveillance of systems, alerting on suspicious activities, and perform initial triage and containment guidance for any security incidents.
- Security Baseline Implementation: Set and enforce security baselines on all Supplier-managed systems. This includes hardened configurations for operating systems, cloud environment guardrails (secure IAM settings and network firewall rules), and ensuring that encryption is enabled by default for data in transit and at rest.
- Vulnerability & Compliance Reporting: Conduct regular vulnerability scans and security assessments. Provide the Buyer with compliance dashboards and reports (e.g. patch status, vulnerability findings, configuration compliance against standards), along with recommended remediation actions.
- CloudSecOps Protection: Manage cloud security posture for any cloud services under Supplier management, integrating with native cloud security tools. Maintain continuous security monitoring and posture dashboards to quickly identify and address misconfigurations or threats in the cloud layer.
- Identity Security: Implement and manage identity lifecycle processes with automated provisioning/deprovisioning and RBAC frameworks. Deploy and operate PAM solutions, including credential vaulting and just-in-time access. Conduct access reviews and attestation reporting whilst managing MFA, SSO, and identity federation services with conditional access policies.
- Consulting Assessment Services: Assess and evaluate security architectures against industry frameworks (NIST, ISO 27001, NCSC), providing gap analysis and roadmaps. Evaluate security maturity levels and regulatory compliance readiness (GDPR, NIS2, Cyber Essentials), delivering risk registers, remediation plans, and measurable recommendations.
- Professional Services: Design and deploy security solutions with comprehensive documentation and knowledge transfer. Implement and configure security platforms (SIEM, endpoint, and cloud) whilst leading transformation initiatives, including SOC modernisation and zero-trust adoption. Deliver training programmes and operational enablement, ensuring sustainable Buyer capabilities.

BUYER RESPONSIBILITIES

- Security Governance & Policy Decisions: Define the organisation's security policies, risk appetite, and governance processes. The Buyer's security leadership sets the acceptable level of risk and must approve any exceptions (e.g., accepting a risk for a temporarily unpatched system).
- Application & Data-Layer Security: Secure any applications, data, or integrations that the Buyer manages. This includes ensuring in-house application code is secure (free of critical vulnerabilities), that APIs are protected, and that sensitive data is properly classified and protected in accordance with the company's policies.
- Remediation Execution: Act on security alerts and recommendations provided by Supplier. The Buyer is responsible for applying patches and remediating vulnerabilities on systems under their control, or scheduling downtime for Supplier to patch managed systems as per the agreed process.
- Identity Governance: Manage the lifecycle of user identities in Buyer-managed directories or applications. This includes onboarding/offboarding users, managing permissions for roles not fully managed by Supplier, and approving elevated access requests. Regularly review user access to ensure compliance with the principle of least privilege.
- Compliance & Audit Coordination: Own regulatory compliance obligations, manage audit requests, and provide necessary evidence/documentation. Ensure third-party suppliers and business partners meet security requirements and maintain contracts with appropriate security clauses.
- Change Management Approval: Review and approve security-related change requests, maintenance windows, and service disruptions. Provide business context for risk assessments and prioritise remediation activities based on business criticality.
- Security Awareness & Training: Ensure end-user security awareness training completion and policy acknowledgement. Maintain acceptable use policies, enforce disciplinary measures for policy violations, and promote a security culture across the organisation.

SUPPLIER SERVICE SPECIFIC TERMS

SECTION 1 – SUPPLIER SLA (GENERAL SLA TERMS)

1. INTRODUCTION

This General SLA, the additional SLA in the Service Definition, and any applicable third-party SLA (as communicated to Buyer and included in the Order Form or the Call-Off Contract) shall collectively constitute the applicable Supplier SLA for the relevant Services.

2. SEVERITY LEVELS

2.1 Unless otherwise set out in the Call-Off Contract, the Supplier will prioritise all Incidents impacting on the Services, acting reasonably, according to the Severity Levels referenced in the Service Definition and taking into account the applicable Shared Responsibility Model for the relevant IaaS, PaaS or SaaS Services.

3. SERVICE LEVELS

3.1 Unless otherwise agreed by the Supplier in the Call-Off Contract, the Supplier shall use its reasonable endeavours to provide the Services in accordance with the relevant Service Levels set out in the Service Definition, subject to the Buyer's compliance with its responsibilities under the Call-Off Contract and any applicable shared responsibility model.

3.2 No Service Credits will apply to the Services unless specifically agreed to by the Supplier in the Call-Off Contract. If any are agreed in the Call-Off Contract, then the mechanism and measurement parameters will be agreed by the Parties. Notwithstanding this, any Service Credits agreed shall:

3.2.1 apply only to a limited number of critical severity Incidents.

3.2.2 be limited to a maximum financial limit proposed by the Supplier and agreed in the Call-Off Contract;

3.2.3 apply only to Incidents solely attributable to the Supplier's fault and not to any failure arising from Buyer-controlled configurations, Buyer Elements or Third-Party Elements; and

3.2.4 constitute the Supplier's sole financial liability for failing to meet the Service Levels for that critical severity Incident.

Any payments made by the Supplier shall be deducted from the overall figure set for the Supplier's limitation of liability. Service Credits (if any) shall constitute the Buyer's sole and exclusive remedy for Service Level failures, save where otherwise expressly required by the Call-Off Contract.

3.3 In the event of a dispute arising between the Supplier and the Buyer over any matter relating to Service Credits, such dispute shall be dealt with in accordance with the dispute resolution procedure set out in the Call-Off Contract.

4. MAINTENANCE

4.1 In order for the Supplier to maintain the performance of the Services, maintenance work must be undertaken by the Supplier from time to time ("**Maintenance**"). Such Maintenance may result in the temporary unavailability of individual functions or components of the Services, or of complete access to the Services, as Maintenance is undertaken. The Supplier shall give the Buyer: reasonable advance notice of planned downtimes where possible; and as much notice as reasonably possible of any unplanned downtimes.

4.2 The Supplier shall use its reasonable endeavours to ensure that any downtime is kept to a minimum and to off-peak times, notwithstanding this (and subject to the following sentence), the Buyer acknowledges and agrees that the Supplier shall not be liable for any downtime of the Services, whether planned or unplanned, whether during peak or off peak times and whatever the duration of such downtime except to the extent such downtime is taken into account for the purposes of calculating Service Levels expressly agreed in the Call-Off Contract. The Supplier shall only be liable for any unplanned downtime to the extent such unplanned downtime is solely as a result of an act or omission of the Supplier.

5 BUYER RESPONSIBILITIES, ASSUMPTIONS AND DEPENDENCIES, SERVICE CONDITIONS AND EXCLUSIONS

5.1 The Buyer shall be responsible and liable at its cost for the responsibilities set out in the Call-Off Contract, including, without limitation:

5.1.2 providing a list of callers authorised to call the Supplier's helpdesk;

5.1.3 ensuring that all authorised callers speak the language that is supported by the Supplier helpdesk. Unless otherwise agreed by the Supplier, this shall be in English;

5.1.4 providing a Buyer contact point that the Supplier shall report to in relation to Severity Level reporting and other reporting requirements;

5.1.5 providing the Supplier with all reasonable assistance necessary for the Supplier to carry out its responsibilities

under the Call-Off Contract, including screen sharing;

5.1.6 unless otherwise agreed by the Supplier, ensuring that all Incidents are logged in English;

5.1.7 ensuring that accurate details of all its End Users and Devices are provided to the Supplier and that the Supplier is updated and provided with any changes thereto promptly;

5.1.8 complying with any support processes (e.g. Incident escalation, standard service requests) defined by the Supplier;

5.1.9 supporting the Supplier's capacity planning process and providing the Supplier with such advance notice as the Supplier shall reasonably require in order to absorb significant and/or unusual changes in load caused by the Buyer's use of the Services, including changes to compute, storage, network or application usage relevant to IaaS, PaaS or SaaS Services;

5.1.10 ensuring that it and its End Users do not access and/or use the Service other than as expressly provided for in the Service documentation provided by Supplier in relation to such Service and the Supplier Terms, including any applicable shared responsibility model;

5.1.11 ensuring that it does not allow access and/or use of the Service by more than the authorised number and/or level of End Users or use of more than the authorised number of Devices as set out in the Call-Off Contract;

5.1.12 ensuring that it or its End Users do not allow any third party to access and/or use the Service;

5.1.13 notify the Supplier immediately of it becoming aware of an Incident through the agreed channels;

5.1.14 provide all data, documentation and/or other information in relation to the Incident and answer all questions raised by the Supplier or Supplier Parties (as the case may be) within the timescales specified by the Supplier or the Supplier Party (as the case may be), or if no timescales are specified, in a timely manner;

5.1.15 ensure that the relevant people (including the person who reported the Incident) are available and contactable by the Supplier or the Supplier Party (as the case may be), in relation to the Incident;

5.1.16 ensure that the relevant people (including the person who reported the Incident) are appropriately experienced and qualified to fulfil any tasks required of them by the Supplier or the Supplier Party (as the case may be), in relation to the Incident and have the requisite delegated authority to make decisions where relevant relating to the Incident;

5.1.17 co-operate and comply with the reasonable instructions of the Supplier or the Supplier Party (as the case may be) to enable the Supplier or the Supplier Party (as the case may be) to proceed uninterruptedly with the performance of the Services and the Resolution of Incidents;

5.1.18 provide the Supplier or the Supplier Party (as the case may be) with all reasonable assistance necessary for the Supplier to carry out its responsibilities under these General SLA Terms and the Call-Off Contract.

5.2 The following Services assumptions and dependencies are made:

5.2.2 authorised callers have the correct skill set, authorisations, etc. to report an Incident and to speak with the Supplier; and

5.2.3 the Supplier may provide a recorded message to callers, at the Supplier's discretion, where the Supplier reasonably deems an Incident requires a recorded message to be provided (e.g. an Incident affecting multiple customers and/or end users), to enable the Supplier to progress resolution of such Incident.

5.3 The Services shall not cover, and the Supplier shall not be responsible for any failure to achieve any Service Levels in relation to, any Incidents arising (directly or indirectly) as a result of:

5.3.2 accident or neglect by the Buyer, any End User or any third party;

5.3.3 any third-party items or services with which the Service is used;

5.3.4 installation, configuration, operation, or use not in accordance with the Supplier's written instructions, applicable documentation, shared responsibility model or Acceptable Use Policy;

5.3.5 access and/or use in an environment, in a manner or for a purpose for which the Service was not designed;

5.3.6 modification, alteration or repair by anyone other than the Supplier or its authorised representatives; or

5.3.7 installation, access and/or use beyond the licensed use;

5.3.8 Buyer Elements, including Buyer-managed configurations, operating systems, applications, data or networks, where applicable under IaaS or PaaS Services; or

5.3.9 any other causes beyond the Supplier's reasonable control.

For the purposes of the Supplier Terms, all such Incidents shall be considered relief events and any work required to resolve such Incidents (if agreed by the Supplier) shall be charged on a time and materials basis at the Supplier's applicable rates under a separate agreement between the Parties.

6 CLOCK STOP

6.1 For the purposes of assessing compliance with the Service Levels and Service Level measures, time during the following periods shall not count towards the Service Levels and shall be treated as time during which the relevant Service was available:

6.1.2 where the Supplier is awaiting a response or information from the Buyer, an End User or a third party (including Supplier Parties) in relation to the matter;

6.1.3 where the Supplier is awaiting the Buyer, an End User or a third party (including Supplier Parties) to implement

any recommended resolution or complete any required tasks in relation to the matter;

6.1.4 where required for resolution of an Incident, the time during which the person who reported the Incident or, in their absence, any person who might reasonably provide information in respect thereof cannot be contacted by the Supplier;

6.1.5 where the Supplier cannot gain access to the relevant site or component(s);

6.1.6 any period of planned or unplanned maintenance (save to the extent any unplanned maintenance is necessary solely as a result of an act or omission of the Supplier);

6.1.7 where the Incident is due to Buyer, End User or third-party default (including, but not limited to, Buyer error, e.g. poor configuration);

6.1.8 where the Incident results from failure of anything beyond the reasonable control of the Supplier, including systemic power outages, internet backbone failures or public utility provider failures ;

6.1.9 where there is an event of Force Majeure; and

6.1.10 time outside of the relevant Supplier helpdesk and support availability windows.

SECTION 2 – SUPPLIER LICENSE TERMS

PART A – SUPPLIER LICENCE TERMS - FOR PAAS OR IAAS

1. USE OF SERVICES

1.1 The Supplier will supply the Services (IaaS and/or SaaS) for use of Buyer as indicated in the Call-Off Contract in accordance with these Supplier Licence Terms. This Part A Supplier Licence Terms – For PaaS or IaaS shall always be read and applied together with Part D Supplier Licence Terms - General Clauses and Part E Supplier Licence Terms - Definitions.

1.2 Subject to and conditional upon full payment by the Buyer of all sums properly due under the Call-Off Contract; and the Buyer's and End Users' compliance with the Supplier License Terms; the Supplier grants to (i) the Buyer, (ii) employees of the Buyer and (iii) the Buyer's suppliers and contractors who require access to the Services solely for the purpose of performing services for the Buyer, a non-exclusive, non-transferable and non-sub-licensable right to access and use the Services and the applicable Supplier Content, during the Term, in an environment hosted by or on behalf of the Supplier, for:

1.2.1 the Buyer's own internal business purposes; and

1.2.2 any other agreed purposes expressly agreed in writing in the Call-Off Contract (the "**Licence**").

1.3 All rights, title, interest and know-how in and to the Services and any Service Elements, and any part or improvement thereof, other than those expressly granted under these Supplier Terms, shall remain wholly vested in the Supplier or its third-party suppliers and/or licensors.

1.4 The Buyer acknowledges and agrees that the Supplier may engage sub-processors in the performance of the Services, including cloud infrastructure and platform providers, and that such sub-processors may engage further sub-processors, subject to compliance with applicable data protection obligations.

1.5 If the Buyer's actual use exceeds the use permitted under the Licence (including in respect of users, volume or capacity), the Buyer shall pay for such excess usage at the Supplier's then-current rates, together with any additional costs reasonably incurred by the Supplier as a result of such excess use, unless otherwise agreed in the applicable Call-Off Contract.

1.6 Where a Call-Off Contract specifies acceptance requirements for any Services, the acceptance provisions set out in Part C shall apply. If no acceptance requirements or criteria are specified, the Buyer shall be deemed to have accepted the Services upon delivery. Unless otherwise expressly agreed in the Call-Off Contract, Services shall be deemed accepted when they are made available for use by the Buyer. Acceptance testing shall not apply to IaaS or PaaS Services unless Cloud Support Services are included and expressly subject to acceptance criteria

1.7 The Buyer shall not, and shall procure that End Users shall not, without the Supplier's prior written consent:

1.7.1 modify, alter or remove any copyright notices, trademarks or other intellectual property notices appearing on or in the Services or Service Elements;

1.7.2 create software products that interface with the Service Elements other than through documented or expressly permitted APIs ;

1.7.3 reproduce, download, copy or remove the Service Elements from the Supplier's systems;

1.7.4 sell, rent, license, sublicense, resell, assign, transfer, distribute or otherwise commercially exploit the Services or Service Elements;

1.7.5 modify, adapt, enhance, repair or create derivative works from the Service Elements;

1.7.6 reverse assemble, disassemble, reverse engineer, decompile or otherwise reduce the Service Elements to human-readable form, except to the extent permitted by applicable law.

1.8 Except for any licence expressly granted under Clause 1.2, all licences granted under this Clause may be suspended or terminated where the Buyer or any End User commits a material breach which is not remedied within a reasonable period following written notice.

1.9 The Supplier shall provide the Services on the agreed timeframe in accordance with the availability levels set out in the applicable Call-Off Contract, except for

1.9.1 planned downtime (which shall be notified in advance); and

1.9.2 emergency or urgent unavailability caused by events beyond the Supplier's reasonable control.

1.10 In order to receive the Services, the Buyer shall take all measures required to receive and use the Services, including, without limitation, the installation, configuration, operation, maintenance and security of Buyer-managed systems, software and on-site equipment. The Supplier shall not be liable for any failure or delay in the provision of the Services to the extent caused by the Buyer's failure to implement such measures or fulfil such responsibilities.

1.11 Unless otherwise agreed, the Supplier shall deliver the Services at the Supplier-managed network interface or virtual network boundary used for the provision of the Services. The Buyer shall, at its own risk and cost, effect the transfer of information from and to the point of delivery of the Services.

1.12 The Buyer shall comply with all applicable laws and regulations in connection with its use of the Services, including those relating to data protection, international communications and the transmission of technical or personal data, and with any reasonable security standards or protocols notified by the Supplier. While using the Services, the Buyer (including its Affiliates and subcontractors) shall not, and shall ensure that any person using the Services under the Buyer's account does not;

1.12.1 harm other persons or infringe their personal rights;
1.12.2 infringe intellectual property or other proprietary rights
1.12.3 impersonate any person or obtain unauthorised access to the Services;
1.12.4 upload or transmit malware or harmful code;
1.12.5 use the Services for any purpose other than as permitted under these Supplier Terms;
1.12.6 transmit, store or upload content to which it is not legally entitled; or
1.12.7 endanger the stability, integrity or security of the Services or underlying infrastructure.

1.13 The Buyer represents and warrants that any user accessing the Services using the Buyer's credentials acts on behalf of the Buyer and accepts the applicable terms of use. The Buyer shall be responsible for the acts and omissions of such users as if they were the Buyer's own acts and omissions and shall defend and hold harmless the Supplier against third-party claims arising from the Buyer's or its users' breach of these Supplier Terms, subject to the limitations of liability set out herein.

1.14 The Parties acknowledge and agree that the provision and use of the Services is based on a shared responsibility model. Except as expressly stated in the Call-Off Contract;

1.14.1 the Supplier is responsible for the security, availability and operation of the underlying cloud infrastructure and Service Elements up to the Service Boundary; and
1.14.2 the Buyer is responsible for the configuration, management, security and lawful use of Buyer Elements, operating systems, applications, data, access controls and network connections beyond the Service Boundary.

1.15 Service Levels, if any, shall apply solely to the availability of the Service Elements at the Service Boundary. Any failure attributable to Buyer Elements, Buyer network connectivity, Buyer configuration or third-party services shall be excluded.

2 UPDATES, UPGRADES, NEW VERSIONS, AND NEW FUNCTIONALITY

2.1 In respect of Service Elements provided as part of the Services, that the Buyer accesses and/or uses as part of, in connection with or as a Service, the Supplier may, but is not obliged to, issue Updates, Upgrades, patches and/or substitute New Versions, which may or may not include any New Functionality thereto at any time at its discretion. The Supplier shall use its reasonable endeavours to notify the Buyer of any material Updates, Upgrades, New Versions or New Functionality and to provide advance notice (as reasonably possible) of any material changes to the Service Elements that may affect any baseline services agreed by the Parties at a certain date to form connectivity to the Buyer Elements.

2.2 The Buyer shall, at its own cost, update, configure or upgrade Buyer Elements, including operating systems, applications and configurations, as reasonably necessary to ensure continued connectivity and compatibility with the Service Elements.

2.3 Updates, Upgrades, New Versions and/or New Functionality which are not required to maintain the existing Services may be subject to additional Charges. Where additional Charges are payable in relation to an Update, Upgrade, New Version or New Functionality, the applicable Charges shall be notified to the Buyer at the time of the issue of the notice in relation to such Update, Upgrade, New Version or New Functionality or in the Charges description relating to the Service.

2.4 Where an Update, Upgrade or New Version materially reduces the core functionality of the Services, and such reduction is not remedied within a reasonable period, the Buyer's sole remedy shall be to terminate the affected Services without penalty

3 SECURITY AND BACK-UP

3.1 The Supplier shall provide and maintain physical, logical and technical safeguards for the protection of the Services and Content in accordance with applicable industry standards for cloud infrastructure services. Such safeguards shall apply up to the Service Boundary and shall not extend to Buyer Elements, except where expressly agreed in the Call-Off Contract.

3.2 The Buyer acknowledges that it is, and shall remain at all times, in control of and solely responsible for Buyer Elements, including its site, and the condition and operation of the facilities, systems and environments under its control.

3.3 The Buyer shall integrate the Services into its overall, state-of-the-art industrial security framework. The Buyer shall ensure that any technical setup, and any amendments or changes made in connection with the Services to its facilities or technical environment (including connectivity for remote access), are aligned with market standards, comply with applicable third-party requirements, and are compatible with the Buyer's IT security policies and individual security requirements.

3.4 The Buyer shall be responsible for reviewing and complying with all applicable laws before first receipt of the Services. In particular, the Buyer shall, at its own expense, obtain and maintain all permits and registrations and fulfil all other legal requirements (including any notification obligations) for data transfer and data processing in connection with the receipt or use of the Services. The Supplier expressly advises the Buyer that the acquisition of the Services may require adaptation or renewal of existing permits. Both Parties agree that the Supplier shall have no obligation to deliver any aspect of the Services that is dependent on Buyer-controlled prerequisites until all necessary requirements have been fulfilled by the Buyer.

3.5 Under no circumstances shall the Buyer transfer any data to the Supplier if such transfer would result in the Supplier breaching applicable law (including export control regulations and laws protecting classified information) or infringing third-party rights by performing the Services. The Buyer is solely responsible for establishing all prerequisites for lawful access to the data from any location where data is accessed.

3.6 The operation of the Service Elements and any Buyer Elements may be unencrypted and involve:
- 3.6.1 transmissions over various networks;
- 3.6.2 changes to conform and adapt to the technical requirements of connecting networks or devices; and
- 3.6.3 transmission to Supplier Parties, including to provide the necessary hardware, software, networking, storage and related technology required to operate and maintain the Service Elements.

3.7 The Supplier shall apply encryption and security controls consistent with generally accepted cloud industry standards for the Service Elements up to the Service Boundary, save where the Buyer has elected or configured otherwise. Accordingly, unless otherwise agreed by the Supplier in the Call-Off Contract or the Service Definition, the Buyer bears sole responsibility for providing and ensuring adequate security, protection, configuration and back-up of Buyer Elements, including data, applications and operating systems.

3.8 Any log-in credentials and private keys provided to the Buyer as part of the Services are for the Buyer's internal use only. The Buyer shall not sell, transfer or sublicense them to any third party.

3.9 The Buyer must promptly notify the Supplier of any suspected misuse of its accounts or authentication credentials, or any actual or suspected security incident related to the Services that may reasonably impact the Service Elements.

4. ENVIRONMENT

4.1 The Buyer shall receive no ownership of or interest in:
- 4.1.1 the Supplier's or any Supplier Party's physical or virtual hardware;
- 4.1.2 any Supplier Content the Supplier or any Supplier Party installs (unless that Content is Buyer Content supplied by the Buyer on the Supplier's or the relevant Supplier Party's physical or virtual hardware);
- 4.1.3 any virtual infrastructure, platform components, or data storage technology the Buyer accesses and/or uses as part of the Services; or
- 4.1.4 the Service Elements.

4.2 Each Supplier-provided virtual computer or platform environment remains the Supplier's or the relevant Supplier Party's exclusive property and accordingly the Buyer shall have no right to download or transfer the Supplier's virtual computer, platform control plane or underlying infrastructure to any other service provider, provided that this clause shall not restrict the Buyer's right to export, migrate or transfer Buyer Elements, including data, virtual machine images, containers or configurations, using standard tools and interfaces.

4.3 Unless otherwise expressly agreed in the Call-Off Contract, the Services may be provided within a shared, multi-tenant environment. The Buyer acknowledges that logical (but not physical) separation of workloads is standard cloud practice or

IaaS and PaaS offerings.

5. BUYER RESPONSIBILITIES

5.1 In addition to any other Buyer responsibilities under the Call-Off Contract, the Buyer is solely responsible and liable at its own cost for:

5.1.1 its, its third parties', its End Users' and the Buyer Element's compliance with all applicable Laws, rules and regulations related to the performance of the Buyer's, its third parties' and any of its End Users' obligations that arise under or in connection with the Call-Off Contract and the Buyer's use of the Services;

5.1.2 its, its third parties', its End Users' and the Buyer Element's compliance with the terms of the Call-Off Contract, these Supplier Terms (including non-violation of the Acceptable Use Policy) and any Third-Party Terms;

5.1.3 ensuring that it, its third parties, its End Users and the Buyer Elements do not cause any loss, destruction, corruption, degradation or other damage to the property or assets (including technical infrastructure) of the Supplier, its lessors or any Supplier Party, the Service Elements, other Content belonging to other customers or any other technical problems;

5.1.4 the protection, compliance and integrity of all Buyer Elements, including without limitation, its accuracy, quality, reliability, appropriateness, development, maintenance, use, back-up, technical operation and compatibility with documented APIs;

5.1.5 obtaining, maintaining and upgrading any Buyer Elements or ancillary services needed to access and/or use the Service Elements (including ensuring any connectivity or compatibility with the Service Elements);

5.1.6 administering security within the Services (e.g. configuring End User access rights), ensuring reasonable security for integration between Buyer Elements and the Service Elements and maintaining the confidentiality of usernames, passwords and other sensitive information relating to the Buyer Account and the Services. The Buyer shall notify the Supplier immediately if the Buyer has reasonable grounds for believing that there has been any unauthorised access to or use of the Buyer Account or the Service Elements or any password or Buyer Account information is lost or stolen or any other known or suspected breach of security relating to Buyer-controlled components;

5.1.7 all activity occurring under the Buyer Account;

5.1.8 discharging its obligations and making decisions relating to the Call-Off Contract in accordance with agreed timescales or if no timescales are agreed in a timely manner and in any event within such time as is required for the Supplier to discharge its obligations under the Call-Off Contract;

5.1.9 providing the Supplier with access to appropriate members of the Buyer's staff, contractors, suppliers, and those of its agents, as may reasonably be required for the Supplier to discharge its obligations under the Call-Off Contract;

5.1.10 providing sufficient, suitable, appropriately qualified, experienced and competent personnel to fulfil the Buyer's roles and duties under the Call-Off Contract;

5.1.11 co-operating fully and procuring that its relevant employees, agents, suppliers and sub-contractors co-operate and comply with the reasonable instructions of the Supplier to enable the Supplier to proceed uninterruptedly with the provision of the Services;

5.1.12 providing the Supplier promptly with all documentation, data and/or other information (including but not limited to, complete and accurate information and instructions upon which the Supplier can rely) concerning its organisation, operations and activities relevant to the Supplier's provision of the Services or that is necessary for the Supplier to perform its obligations under the Call-Off Contract and when requested by the Supplier, shall promptly provide answers to any reasonable questions from the Supplier. The Buyer shall inform the Supplier of any information or developments which may come to the Buyer's notice, and which might have a bearing on the Services;

5.1.13 the Buyer agrees that the Supplier may receive data, information and material from the Buyer or from other sources in the course of delivering the Services and that the Supplier shall not independently investigate or verify such documentation, data and/or other information and that the Supplier shall be entitled to rely upon the accuracy and completeness of such documentation, data and/or other information in performing the Services. The Supplier shall not be liable to the Buyer or any End User for any loss or damage suffered by the Buyer or any End User arising from fraud, misrepresentation, withholding of documentation, data and/or other information related to the Services or other default relating to such documentation, data and/or other information, whether on the Buyer's part or that of the other information sources;

5.1.14 notwithstanding the Supplier's duties and responsibilities in relation to the Services, the Buyer shall retain responsibility and accountability for: (i) the management, conduct and operation of its business and affairs; (ii) determining its use of, the extent of its reliance on, and any implementation of, the Supplier's advice or recommendations or any other product of the Services supplied by the Supplier; (iii) making any decision affecting the Services, any product of the Services, its interests or its affairs; and (iv) the delivery, achievement or realisation of any benefits directly or indirectly related to the Services which require implementation by the Buyer;

5.1.15 where the Services include on-site Cloud Support Services, the Buyer shall ensure that all arrangements are made for access (including for the avoidance of any doubt to national and international networks as the Supplier may reasonably require), security procedures, virus checks, facilities (including without limitation desks, access to telephone lines, analogue lines, fax, photocopying and printing and GRA VPN facilities) as may be required. The

Buyer accepts that the Supplier may use either the Buyer's network or dial-up facilities to access the Supplier's own network and that the Buyer has assessed and accepts any associated risks which may arise;

5.1.16 where applicable, the Buyer shall afford to the Supplier and Supplier Parties full and safe access to the Buyer premises. The Buyer shall advise the Supplier in writing of all rules, regulations, policies and procedures in place at the Buyer premises relating to health, safety or security, and the Supplier shall ensure compliance by Supplier Parties with all such reasonable and lawful rules, regulations, policies or procedures of which it is notified in writing;

5.1.17 unless otherwise expressly agreed in the Call-Off Contract, the Buyer remains solely responsible for implementing and maintaining appropriate back-up, retention and recovery procedures for its data and applications, and the Supplier shall not be responsible for backing up Buyer Content or Buyer Elements.

5.1.18 where the Buyer orders business continuity and/or disaster recovery services as part of the Services, the scope and details of such services shall be set out expressly in the Call-Off Contract or the applicable Service Definition. Any amendment required to be made by the Supplier to its own business continuity and disaster recovery plans in order to align with or comply with the Buyer's plans shall be implemented at the Buyer's cost. (Any business continuity or disaster recovery services provided by the Supplier shall apply solely to the Service Elements and shall not extend to Buyer Elements, Buyer Content, applications, operating systems or configurations, unless expressly stated otherwise in the Call-Off Contract); and

5.1.19 other than any licences, authorities, approvals and consents required to be provided by the Supplier as part of the Services, obtaining and maintaining throughout the Term of the Call-Off Contract all necessary licences, authorities, approvals and consents required to permit the Supplier and Supplier Parties to perform the Services and the Buyer to receive the Services and/or that may be required in relation to the Buyer Elements (including any that may be required for the use of such Buyer Elements with the Service Elements).

6. END USERS AND DEVICES

6.1 Unless otherwise agreed by the Supplier in the Call-Off Contract, the Buyer shall provide the Supplier with a list of End Users and/or, where applicable to the Service, authorised user accounts, identities, roles, service accounts, service principals or API credentials to be permitted access to and/or use of the Buyer Account and the Services under the Call-Off Contract, where such identification is required by the applicable Service.

6.2 The Supplier shall, where relevant to the Service, provide the Buyer with a list of supported or compatible Devices or other supported access methods, interfaces, endpoints, operating environments or client configurations, as applicable, that may be used with the Service.

6.3 The number of End Users and/or authorised user accounts, identities, roles, service accounts, service principals or API credentials, as applicable to be permitted access to and/or use of a Service and the number of Devices or other applicable access methods or endpoints that may be used with a Service shall be set out in the Charges description relating to the Service or, where relevant, the applicable usage, capacity or consumption limits for the Service.

6.4 Should the Buyer wish to add additional End Users or Devices, or increase the number of authorised accounts, identities, access methods or applicable usage, capacity or consumption limits over and above the number permitted with respect to the Services ordered, it shall lodge a request with the Supplier and, where the Supplier agrees to such addition or increase, the Buyer shall inform the Supplier in writing of the relevant details and pay the applicable additional Charges.

6.5 Charges relating to additional End Users and/or Devices or other applicable access, usage, capacity or consumption increases over and above the number allowed with respect to the Service ordered are set out in the Charges description relating to the Service or, if not set out in the Charges description relating to the Service shall be notified to the Buyer at the time of such request.

PART B – SUPPLIER LICENSE TERMS - FOR SAAS

1 DEFINITIONS & INTERPRETATION

1.1 In this Part B the following words shall have the following meanings:

Term	Definition
"Additional Charges"	means charges for any Chargeable Work and/or in respect of any excess usage of the Subscription Services, which shall be calculated in each case in accordance with the Supplier's standard time and materials rates or excess usage charges (as applicable) from time to time.
"Authorised User"	in respect of a Subscription Service means a client who is authorised by the Buyer to use that Subscription Service in accordance with the Call-Off Contract.
"Available"	means that the relevant Subscription Service is available for access at the Service Boundary. A Subscription Service shall not be treated as unavailable to the extent that any inability to access it results from defects or errors in the Buyer Network Equipment or any other matter outside of the Service Boundary.
"Chargeable Work"	means any of the work described in Clause 6.2 of this Part B and any work that the parties agree in writing that the Supplier shall perform that does not form part of the then current Services.
"Client"	means, depending on the type of functionality which the Server Software provides, an individual user, agent, item of equipment, device, identity or communication channel or similar logical or physical endpoint.
"Client Software"	means that part of the Subscription Software (if any) that is designed to be installed on individual end user devices (such as, without limitation, a mobile phone, laptop, PC or tablet) to enable remote access to and use of the functionality provided by that part of the Subscription Software that is installed on one or more of the Supplier's servers.
"Buyer Contract Manager"	means the Buyer's management point of contact for the Supplier as notified by the Buyer to the Supplier from time to time.
"Buyer Network Equipment"	means any of the Buyer's (or its third-party suppliers') IT and telecommunications infrastructure, including personal computers, mobile devices, data network equipment, telecommunications networks and all associated equipment that is either: (i) used to access the Subscription Software or with which the Subscription Software is to inter-operate; and/or (ii) used by the Supplier to provide the Services, as the case may be.
"Buyer Support Representatives"	means such of the Buyer's representatives as are authorised in writing from time to time by the Supplier to report Incidents to the Supplier.
"Downtime"	means any time during Service Hours when the relevant Subscription Service is not Available, excluding Scheduled Downtime.
"Incident"	means an operational event which is not part of the standard operation of the Subscription Software and/or Service(s), but excluding any such event that results from or constitutes a Service Exclusion or is caused by the failure of a Service Dependency.
"Maximum Capacity"	in respect of any item of Subscription Software, means the maximum capacity for that Subscription Software as set out in the Service Definition applicable to that Subscription Software and/or as notified in writing by the Supplier to the Buyer from time to time.
"Network Operator(s)"	means a public or private telecommunications operator providing a network or services that is regulated by a licence granted under the Telecommunications Act 1984 or any successor legislation.
"Scheduled Downtime"	means any period of Downtime that is scheduled in advance by the Supplier for the purposes of carrying out maintenance to or upgrading of or other work in respect of the Subscription Services or any equipment or systems on or with which it operates.
"Server Software"	means any part of the Subscription Software that does not comprise Client Software and includes each element of the Subscription Software that is designed to be hosted on the Supplier's servers and is not intended to be installed on individual end user devices (such as, without limitation, a mobile phone, laptop, PC or tablet).
"Service Boundary"	in respect of each Subscription Service shall have the meaning ascribed to it in the relevant Service Definition but if not otherwise defined shall mean the point at which the Supplier's (or its sub-contractor's) hosted solution initially connects to the Internet or any telecommunications network.
"Service Commencement Date"	in respect of each Service means the date that Supplier first makes that Service available to the Buyer.
"Service Dependencies"	in respect of each Service means the matters, things and/or activities on which that Service is dependent for its successful operation or performance, as identified under in the Service Definition or elsewhere in the Call-Off Contract.
"Service Exclusion"	means any exclusion from the Services that is specified in the Service Definition or elsewhere in the Call-Off Contract. It shall also include any defect or error or loss of service caused by anything outside of the Service Boundary for the Service concerned.

"Service Hours"	in respect of a Service means the contracted service hours during which that Service is to be made available as set out in the Service Definition.
"Service Implementation"	means the implementation of the service identified as such (if any) in the Service Definition and in Clause 2.1 of this Part B.
"Site(s) "	means the Buyer site(s) identified in the Call-Off Contract as varied from time to time by written agreement with Supplier, such agreement not to be unreasonably withheld or delayed.
"Subscription Services"	means the subscription services provided or made available by the Supplier to the Buyer under the Call-Off Contract, as more particularly described in the relevant Service Definitions
"Subscription Service Usage Restrictions"	in respect of each Subscription Service means the restrictions on usage of the Subscription Services (and associated Subscription Software) specified in the relevant Service Definition.
"Subscription Software"	means the software described as such in the Call-Off Contract (including the software for the provision of SAAS) as varied from time to time in accordance with the Call-Off Contract.
"Supported Equipment"	means the Buyer's equipment (if any) identified under that title in the Call-Off Contract in respect of which Supplier agrees to provide Support Services.
"Support Services"	means the services (if any) described as such in the Call-Off Contract as described in more detail in the relevant Service Definition.
"Supplier's Call Desk"	means the Supplier's help desk, the contact details of which are provided by the Supplier to the Buyer from time to time.
"Supplier Equipment"	means the equipment (if any) which Supplier installs on any Site for Supplier's use for the provision of the Services.
"Supplier Software"	means the software element of Supplier Equipment.
"Upgrade/upgrade"	means a major release of software, denoted by a change to its initial version number.
"User"	means any user of the Subscription Services or Web Tools who obtains access to such Subscription Services or Web Tools, whether or not they are authorised to do so. It includes any person that communicates with the Buyer through the use of the Subscription Services.
"User Subscriptions"	means the user subscriptions purchased by the Buyer pursuant to the Call-Off Contract, which entitle Authorised Users to access and use the relevant Subscription Service (including relevant Subscription Software) in accordance with the Call-Off Contract.
"Web Tools"	means the web tools made available for use by the Supplier with the Services from time to time and any changes to them notified to the Buyer in writing by the Supplier from time to time

2 SUPPLY OF SERVICES

2.1 The Supplier will supply the Services (SaaS) for the Buyer's use as indicated in the Call-Off Contract and in accordance with these Supplier Licence Terms, and this Part B (Supplier Licence Terms – SaaS) shall always be read and applied together with Part D (Supplier Licence Terms – General Clauses) and Part E (Supplier Licence Terms – Definitions).

2.2 Subject to the Service Dependencies and any Service Exclusions, Supplier shall provide the Service Implementation to the extent applicable to the configuration, onboarding, activation or enablement of the Subscription Services following signature of the Call-Off Contract and shall provide or make available the other Services from their respective Service Commencement Dates during any Service Hours whether such Subscription Services are hosted by the Supplier or by a third-party hosting provider engaged by or on behalf of the Supplier.

2.3 Subject to Clauses 2.2 and 2.3 of this Part B and to the other exceptions and exclusions set out elsewhere in the Call-Off Contract, Supplier shall use reasonable endeavours to provide the Subscription Services as a hosted software-as-a-service solution, including where the hosting environment is provided by a third party in accordance with the Service Levels applicable to them.

2.4 Supplier shall use reasonable endeavours to make the Services available from the target start dates for them agreed in writing by the Parties, acknowledging that such dates are indicative only and may be dependent on completion of Buyer onboarding activities and the availability of any third-party hosting services, but such dates are estimates only and Supplier shall not be liable for any failure to meet them.

2.5 It shall be a Service Dependency for all Subscription Services delivered on a SaaS basis which are dependent upon the Buyer Network Equipment that the Buyer Network Equipment is sufficient to facilitate access to and use of the Services via supported browsers, client applications or network connections in accordance with the Call-Off Contract and that it is in full working order regardless of whether the Services are hosted by the Supplier or a third party.

2.6 Scheduled Downtime shall be excluded from any Availability calculations for the purposes of assessing performance against any Service Levels. However, Supplier shall use reasonable endeavours to keep any Scheduled Downtime to a minimum

and to undertake maintenance outside of Service Hours wherever reasonably practical, wherever reasonably practical, including routine maintenance, upgrades and patches to the SaaS platform or the underlying third-party hosting environment, and where reasonably practicable shall provide advance notice of Scheduled Downtime including where such downtime arises from third-party hosting activities.

2.7 Time shall not be of the essence in respect of performance by Supplier of its obligations, including the provision, configuration or availability of the Subscription Services, whether hosted by the Supplier or a third party.

2.8 Telephone calls to and from Supplier's Call Desk may be recorded for training, quality assurance and security purposes.

3 BUYER'S OBLIGATIONS

3.1 The Buyer acknowledges that the Subscription Services have been selected by the Buyer relying solely on its own judgement as to their fitness and suitability for its purposes.

3.2 The Buyer shall:

3.2.1 ensure that any Incidents are promptly reported in adequate detail to Supplier. The Buyer shall ensure that Incidents are reported to Supplier and that all communications with Supplier's Call Desk are made only by the Buyer Support Representatives and not by any other individual;

3.2.2 ensure that the Buyer Contract Manager is available to Supplier as reasonably required by Supplier to facilitate provision and/or availability (as the case may be) of the Services;

3.2.3 ensure that it has and maintains in force all licences, consents, and permissions necessary for the performance of its obligations under the Call-Off Contract;

3.2.5 ensure that Supplier has such reasonable remote access to Buyer systems, accounts or environments as is necessary for the provision of the Services, where expressly agreed in the Call-Off Contract;

3.2.6 ensure that it and those for whom it is responsible do not hinder or interrupt Supplier's provision of the Services;;

3.2.7 promptly supply Supplier with such information as Supplier reasonably requires, and ensure that it is accurate, complete and not misleading and shall ensure that subsequent significant changes to it are notified promptly to Supplier;

3.2.8 ensure that all equipment, databases, access keys and other items upon which Supplier is reliant in order to provide the Services in accordance with the Call-Off Contract, and which it is not the responsibility of Supplier to provide under the Call-Off Contract, are provided in a timely manner and maintained in the condition necessary to facilitate provision of the Services by Supplier in accordance with the Call-Off Contract;

3.2.9 ensure that all of the Service Dependencies are fulfilled in a timely manner;

3.2.10 notify Supplier in writing of any planned changes to the Buyer Network Equipment or Buyer Environment which may affect the Services; and allow Supplier to measure the Buyer's usage of the Subscription Services remotely. If this is for any reason not possible or Supplier requests the Buyer to provide usage reports for any reason, the Buyer shall, on or before the 10th calendar day of each month, report to Supplier all usage of the Subscription Services for the preceding month in the manner and in the format reasonably required by Supplier. The Buyer shall ensure that the information contained in these reports is complete, accurate and not misleading.

3.3 All obligations that End Users must comply with or that the Buyer must procure that End Users comply with, as set out in the Supplier Terms, shall also apply to Users, and the Buyer shall ensure that Users comply with such obligations.

4 END USERS AND DEVICES

4.1 Unless otherwise agreed by the Supplier in the Call-Off Contract, the Buyer shall provide the Supplier with a list of End Users, including named users, user types or roles, where applicable, to be permitted access to and/or use of the Buyer Account and the Services under the Call-Off Contract, where such identification is required by the applicable Service.

4.2 The Supplier shall, where relevant to the Service, provide the Buyer with a list of supported or compatible Devices, including supported operating systems, browsers or client applications that may be used with the Service.

4.3 The number of End Users, including any applicable categories, tiers or roles of End Users to be permitted access to and/or use of a Service and the number of Devices, where applicable, that may be used with a Service, shall be set out in the Charges description relating to the Service. Should the Buyer wish to add additional End Users or Devices or upgrade the applicable user tier, role or licence type over and above the number permitted with respect to the Services ordered it shall lodge a request with the Supplier.

4.4 Should the Supplier agree to the addition of such additional End Users and/or Devices or upgraded user tiers, roles or licence types the Buyer shall inform the Supplier in writing of the details of such End Users and/or Devices [or relevant licence details and pay the relevant Additional Charges.

4.5 Charges relating to additional End Users and/or Devices or upgraded user tiers, roles or licence types over and above the number allowed with respect to the Service ordered are set out in the Charges description relating to the Service or, if not set out in the Charges description relating to the Service shall be notified to the Buyer at the time of such request.

5 CHANGE TO SUBSCRIPTION SERVICES

5.1 Supplier shall be entitled to change the Subscription Services and their related Service Definitions in accordance with the terms of Call-Off Contract to reflect any change that Supplier makes generally to its standard subscription service offering from time to time, provided that such changes do not materially reduce the core functionality of the Subscription Services and are implemented in accordance with Clause 13 (Software Releases and Web Tools).

6 CHARGEABLE WORK

6.1 The Buyer shall pay the Additional Charges for all Chargeable Work.

6.2 Chargeable Work shall include all work in connection with, or as a result of:

- 6.2.1 meeting a change in the requirements of any relevant authority applicable to the Buyer's use of the Subscription Services
- 6.2.2 loss of Buyer-generated data, save where due to Supplier's negligence;
- 6.2.3 errors or omissions in information supplied by the Buyer upon which Supplier has relied;
- 6.2.4 Incidents existing prior to the Service Commencement Date;
- 6.2.5 updating or installation of virus protection software within Buyer-controlled environments, save where it constitutes part of the Subscription Services;
- 6.2.6 work which is identified as or is caused by or required as a result of a Service Exclusion, any failure of any Service Dependency and/or any virus or other electronic contaminant introduced by or any denial of service or other system attack instigated by any person other than Supplier and Supplier's contractors;
- 6.2.7 any work to investigate any issue with any Subscription Services that is reported by the Buyer where it is determined by Supplier that there is no defect or error in the Subscription Services or Supported Equipment;
- 6.2.8 any breach of the Buyer's obligations under the Call-Off Contract or any other agreement the Buyer has with Supplier;
- 6.2.9 any defects or errors in the Buyer Network Equipment or Buyer Environment, save where these are themselves caused by Supplier's negligence; and/or
- 6.2.10 Services taking longer or attracting additional costs as a result of any of the above causes or the carrying out of excluded Services.

6.3 The Buyer shall pay Additional Charges if, at any time whilst using the Services, the Buyer exceeds the maximum amount of storage space specified by Supplier in the Call-Off Contract (if any). Such Additional Charges will be calculated in accordance with Supplier's then current standard excess data storage fees as set out in the Charges Schedule or Order Form.

7 TITLE OF SUBSCRIPTION SOFTWARE

7.1 The Buyer acknowledges that it acquires no legal or beneficial ownership in Supplier Equipment or the Subscription Software whatsoever.

8 WARRANTY EXCLUSIONS

8.1 The Subscription Software cannot be tested in every possible permutation and accordingly Supplier does not warrant that the Subscription Services (or the Subscription Software used to provide it) will be free of all defects or that their use will be wholly uninterrupted.

8.2 The Supplier shall not be liable to the Buyer to correct any defect or failure that derives from:

- 8.2.1 any modification or customisation of the Client Software by or on behalf of the Buyer other than by Supplier and/or Supplier's subcontractors or with Supplier's express fully informed prior written approval;
- 8.2.2 failure by the Buyer, its agents and/or other contractors to properly maintain the Client Software (except where and to the extent that this results from any failure by Supplier or Supplier's subcontractors to perform any maintenance that it is obliged to provide as part of the Services);
- 8.2.3 use of the Subscription Services in contravention of Supplier's instructions or use other than for its designed purpose or in excess of their Maximum Capacity;
- 8.2.4 defects or errors in the Buyer Network Equipment or Buyer Environment(save where these were themselves caused by Supplier's negligence) or any matter that is external to the Services themselves;
- 8.2.5 any virus or other electronic contaminant introduced by or any denial of service or other system attack instigated by any person other than Supplier and Supplier's contractors;
- 8.4.5 failure of any Service Dependency; or
- 8.4.6 any Service Exclusion, any breach of the Buyer's obligations under the Call-Off Contract or any matter for which Supplier is excused from liability under any other provision of the Call-Off Contract.

8.3 Notwithstanding the other terms of this Clause 8, but except to the extent that Supplier may not exclude or limit its liability in

law, Supplier provides no warranty, condition or representation in respect of any Open Source Software programs contained in the Subscription Software and such Open Source Software shall be provided by Supplier "as is". The Open-Source Software licences will define the warranty, if any, from the authors or licensors of the Open Source Software. Without prejudice to the generality of the foregoing, Supplier specifically disclaims any warranties, conditions, representations or any other commitments in respect of defects caused by altering any Open Source Software program. Supplier shall not be liable for any claim or allegation that the Open Source Software infringes the intellectual property rights of a third party.

9 SOFTWARE LICENCES

9.1 Certain Subscription Services may include limits on the numbers or identities of Clients or other Subscription Service Usage Restrictions. Where these apply in respect of a particular Subscription Service, the Buyer shall comply with (and ensure that all persons accessing the Subscription Services through the Buyer shall comply with) such limits and Subscription Service Usage Restrictions as set out in the Order Form or applicable Service Definition.

9.2 The Buyer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Subscription Software and/or the Subscription Services and, in the event of any such unauthorised access or use, the Buyer shall promptly notify Supplier and cooperate with Supplier to mitigate the effects of such unauthorised access or use.

9.3 Any technological measures in the Subscription Software that are designed to prevent unlicensed or illegal use of the Subscription Services may not be removed, circumvented or interfered with, and the Buyer agrees to the use by Supplier and/or its licensors of such measures solely for licence compliance, security and integrity purposes.

9.4 Supplier and/or its licensors shall be entitled to automatically check the version level of the Subscription Software and/or their components that are being used by the Buyer including through automated means typical for SaaS Services, provided that such checks do not materially interfere with the Buyer's use of the Services.

9.5 If the Buyer requires information necessary to achieve the interoperability of the Client Software with other programs, it should contact Supplier. Any such information which is provided by Supplier shall only be used by the Buyer to achieve such interoperability, and for no other purpose, and "interoperability" has the meaning within Section 50B of the Copyright Designs and Patents Act 1988.

9.6 Notwithstanding any other provision in the Call-Off Contract to the contrary, any Subscription Software and/or Subscription Services that are subject to click-wrap or click-on licence terms and conditions, are subject to Open Source Software licences, or any other end user licence terms shall be subject to those terms. Such terms will be communicated to the Buyer or stated, by way of hyperlink or otherwise, in the Order Form of the Call-Off Contract.

9.7 Where Subscription Software is subject to click-on or click wrap licence terms, the Buyer hereby authorises Supplier to accept such terms on its behalf and accepts responsibility in respect thereof, provided that the Buyer has been notified of the existence of such terms or such terms have been stated, by way of hyperlink or otherwise, in the Order Form

.

9.8 Certain Subscription Software will require the Buyer to input access codes and/or licence keys in order to obtain full access to it. If and to the extent that Supplier provides activation codes or licence codes under the Call-Off Contract, the Buyer shall keep these confidential and shall not disclose these codes to third parties. In addition where any Subscription Software requires a password to access it then the Buyer shall: (i) ensure that any passwords it is required to create are created with reasonable care and skill in line with current good IT security practice, and (ii) keep all such passwords confidential and not disclose them to third parties.

9.9 Client Software will be supplied in object code only. The source code will not be provided, save where and to the extent that any Open Source Software licence mandates otherwise in respect of it. For the avoidance of doubt, no software code relating to Server Software or the Subscription Services platform will be made available to the Buyer under the Call-Off Contract.

10 USE OF THE SERVICES AND THE WEB TOOLS

10.1 The Buyer shall use the Services and the Web Tools solely for the Buyer's own internal business purposes and not for any other purpose (and in particular the Buyer shall not resell the Services in any manner). The Buyer warrants that it shall not and it shall procure that all Users shall not:

10.1.1 access, store, distribute or transmit any material during the course of the use of the Services or the Web Tools that:

(a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; or is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

(b) depicts sexually explicit images; or

(c) promotes unlawful violence; or

(d) causes or may cause damage or injury to any person or property,

10.1.2 hack into the Services and/or the Web Tools or any linked systems;
10.1.3 interfere with or seek to corrupt or alter any software accessible through the Services and/or the Web Tools;
10.1.4 introduce or cause to be introduced any computer virus or other electronic contaminant into the Services and/or Web Tools or any linked system site;
10.1.5 disrupt or interfere with any part of the Services and/or the Web Tools or any linked systems;
10.1.6 use the Services and/or Web Tools in any way which does or could materially impair or interfere with the use of the Services by any other customer; or
10.1.7 disclose any password or account details which are provided to it under or in connection with the Call-Off Contract (or which it is required to create to use the Service or Web Tools) to any other person or company.

10.2 The Buyer shall, and shall procure that all Users shall, comply with Supplier's Acceptable Use Policy in relation to the Services and the Web Tools as notified by Supplier to the Buyer from time to time, provided that any material changes to such policy shall be notified to the Buyer in advance where reasonably practicable.

10.3 Supplier reserves the right, without liability or prejudice to its other rights to the Buyer, to suspend and/or disable the Buyer's access to the Subscription Services or any particular materials in the event Supplier reasonably considers that there has been a breach of the provisions of above Clause 10.1 and/or to remove any material that Supplier considers may breach the provisions of above Clause 10.1. Where reasonably practicable, Supplier shall provide advance notice of any such suspension or removal and shall take reasonable steps to minimise disruption to the Buyer's use of the Services.. The Buyer shall, and shall procure that the Authorised Users shall, comply with Supplier's reasonable requests in relation to the Buyer's access and use of the Services and/the Web Tools.

10.4 Upon termination of the Call-Off Contract the Buyer shall return or destroy at the option of Supplier all Confidential Information related to the Services and the Web Tools save for Buyer Content and any information the Buyer is required by law to retain.

10.5 The Buyer shall defend and hold harmless Supplier against all claims, actions, proceedings, losses, damages, expenses and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Buyer's use of the Subscription Software and/or Services except where and to the extent caused by the Supplier's breach of the Call-Off Contract, negligence or deliberate misconduct.

10.6 Supplier shall not be responsible for (howsoever arising):
10.6.1 modifications made to the Services and/or the Web Tools by persons other than Supplier or Supplier's contractors;
10.6.2 damage by a computer virus or other electronic contaminant to the Services and/or the Web Tools originating from Buyer
10.6.3 hacking into the Services and/or the Web Tools by any third party except where directly attributable to Supplier's failure to comply with its agreed security obligations;
10.6.4 temporary bandwidth congestion causing problems of access to the Services and/or the Web Tools ;
10.6.5 interruption of internet connection; or
10.6.6 any unlawful or unauthorised monitoring of telecoms traffic by the Buyer or its End Users.

12 DATA PROTECTION AND USE

12.1 The Buyer warrants that it is permitted to provide Supplier with Personal Data and that it has in all respects complied with its obligations under the Data Protection Legislation. The Buyer authorises the Supplier to store Buyer Content and any Personal Data contained within it solely to the extent technically necessary for the provision, operation, support and improvement of the Services within Supplier-controlled environments, where applicable.

12.2 The Supplier may compile statistical and other information relating to the performance, operation and use of the Services from Buyer Content and service usage data, provided that such information is aggregated and anonymised so that it does not constitute Personal Data, for the purposes of security and operations management, service monitoring, benchmarking, analytics, and the improvement of the Services.

12.3 The Supplier may make such aggregated and anonymised information publicly available, provided that it does so only in a manner that does not identify the Buyer, any End User or any individual and cannot reasonably be re-identified. The Supplier shall retain all Intellectual Property Rights in such aggregated and anonymised statistical and performance information.

13 SOFTWARE RELEASES AND WEB TOOLS

13.1 In execution of the Services or delivery of the Subscription Software, Supplier may supply and install a later release of the Subscription Software that may incorporate corrections, bug fixes, security patches and performance improvements. It may also include new features and functionality which, unless agreed otherwise in the Call-Off Contract or elsewhere in writing,

shall be chargeable at Supplier's standard charges, provided that such releases do not materially reduce the core functionality of the Subscription Services.

13.2 Supplier may make Web Tools available to the Buyer from time to time for use with the Services. These Web Tools do not form part of the Services themselves and Supplier makes them available on an 'as is' and 'as available' basis. Supplier reserves the right to change, withdraw or terminate access to the Web Tools at any time in Supplier's sole discretion, provided that such change, withdrawal or termination does not materially affect the Buyer's ability to use the Subscription Services.

PART C – SUPPLIER LICENCE TERMS - CLOUD SUPPORT SERVICES

CLOUD SUPPORT SERVICES

1. INTRODUCTION

1.1 Where the Services ordered by the Buyer include or are solely Cloud Support Services relating to IaaS, PaaS and/or SaaS Services, the provisions set out in this Part C (Cloud Support Services) apply to that part of the Services comprised of the provision of such Cloud Support Services. This Part C shall always be read and applied together with Part D (Supplier Licence Terms – General Clauses) and Part E (Supplier Licence Terms – Definitions.

2. SCOPE OF THE SERVICES AND CLOUD SUPPORT SERVICES DELIVERABLES

2.1 The Call-Off Contract will detail the Services ordered by the Buyer which are Cloud Support Services and any Cloud Support Services Deliverables to be provided thereto. The Supplier will deliver the ordered Services which are Cloud Support Services in accordance with the relevant Service Definition and the relevant shared responsibility model for the applicable IaaS, PaaS or SaaS Services.

2.2 Any support and maintenance services to be provided shall be set out in the Call-Off Contract.

2.3 For that part of the Services that consist of the provision of the Cloud Support Services, the definition of "Service Elements" in Part D of the Supplier Licence Terms shall include the Cloud Support Services Deliverables and Part A of the Supplier Licence Terms shall be construed accordingly.

3. TIMESCALE

3.1 Where the Parties have agreed to an implementation plan and/or an exit plan and off-boarding plan in the Call-Off Contract, the Supplier shall use its reasonable endeavours to meet the implementation plan and/or exit plan and off-boarding plan and milestone dates (if any) agreed with the Buyer in the Call-Off Contract. The implementation plan and/or exit plan and off-boarding plan and milestone dates are subject to any assumptions and dependencies the Supplier has raised with the Buyer and to the Buyer's compliance with the Buyer responsibilities including responsibilities allocated to the Buyer under the applicable cloud shared responsibility model.

4. ACCEPTANCE

Cloud Support Services Deliverables that are software

4.1 When the Supplier has completed any separate Cloud Support Services Deliverables, and the Buyer and the Where the Supplier has completed any Cloud Support Services Deliverables, and the Parties have agreed in the Call-Off Contract that such Deliverables shall be subject to Acceptance Testing, the Buyer may, with the Supplier's reasonable cooperation, conduct Acceptance Tests to verify whether the Cloud Support Services Deliverables substantially conform to the applicable Specifications. Acceptance testing shall be conducted within five (5) days of delivery of the relevant Cloud Support Services Deliverable (or such other period as agreed) (the **"Acceptance Period"**). If the Buyer notifies the Supplier of a Non-Conformity within the Acceptance Period, the Supplier shall use reasonable endeavours to correct the Non-Conformity and notify the Buyer when complete. The Buyer shall then have five (5) days to re-test (the **"Further Acceptance Period"**). If the same Non-Conformity recurs, the Supplier shall work diligently to remedy it. The Parties may agree that certain Non-Conformities may be corrected post-Acceptance. The Supplier's maximum liability for failure to correct a Non-Conformity shall be limited to refunding the fees paid for the non-conforming Cloud Support Services Deliverable (or relevant portion).

4.2 The Buyer shall not withhold or delay Acceptance where any defect is a Minor Defect that does not materially prevent use of the Cloud Support Services Deliverable for its intended purpose.

4.3 Where a Non-Conformity arises from:

- 4.3.1 any act or omission of the Buyer;
- 4.3.2 inaccurate or incomplete information supplied by the Buyer;
- 4.3.3 Buyer breach of its obligations;
- 4.3.4 failure or limitation of third-party platforms, cloud infrastructure or services;
- 4.3.5 incorrect assumptions or dependencies;
- 4.3.6 Buyer Elements; or

4.3.7 the performance or configuration of the Buyer's systems,

the Supplier shall not be responsible for such Non-Conformity, and the Buyer shall accept the Cloud Support Services Deliverable and pay the Charges due. At the Buyer's request and cost, the Supplier may propose remedial work, which may include a workaround or Specification change.

4.4 A Cloud Support Services Deliverable shall be deemed accepted on the earliest of:

4.4.1 expiry of the Acceptance Period without notification of Non-Conformity;

4.4.2 completion of Acceptance Tests where Clause 4.3 applies;

4.4.3 Buyer material default in Acceptance Testing;

4.4.4 use of the Cloud Support Services Deliverable other than for testing; or

4.4.5 instruction to use the Cloud Support Services Deliverable in a live environment.

All other Deliverables

4.5 All other Cloud Support Services Deliverables, including advice, reports, configurations, or recommendations, shall be deemed accepted upon delivery.

4.6 Where delivery, installation or Acceptance Testing is prevented by Buyer default or third-party failure, Charges due upon delivery or Acceptance shall become payable upon Supplier notification of readiness.

4.7 Accepted Cloud Support Services Deliverables shall be deemed approved for subsequent stages. Without prejudice to the Buyer's rights under the Call-Off Contract, the Buyer may bring claims for latent defects later identified.

4.8 The Supplier gives no warranty that any system, configuration or software forming part of a Cloud Support Services Deliverable will be error-free, uninterrupted or capable of correction. The Buyer acknowledges that cloud services are dependent on third-party infrastructure and platforms**.**

5. RISK OF LOSS

5.1 Where Cloud Support Services Deliverables are intangible (including advice, documentation, configurations or scripts), no transfer of risk shall apply. Any physical Deliverables (if applicable) shall transfer risk upon delivery.

6. INTELLECTUAL PROPERTY RIGHTS

6.1 In relation to Cloud Support Services Deliverables, the Supplier grants the Buyer a worldwide, revocable, non-exclusive, non-transferable, non-sub-licensable licence to use the Cloud Support Services Deliverables solely for the Buyer's internal business purposes in connection with the supported IaaS, PaaS or SaaS Services.

7. MAINTENANCE AND SUPPORT SERVICES

7.1 Supplier shall provide Maintenance and Support Services (if any) in accordance with the Call-Off Contract or Order Form, specifying the supported cloud services or components.

7.2 Unless otherwise stated in the Call-Off Contract, the Maintenance and Support Services shall be provided during the Supplier's normal working hours.

7.3 The Maintenance and Support Services may include:

7.3.1 support relating to cloud configurations, platform usage, integrations and software components; and/or

7.3.2 corrective maintenance through patches or Updates provided by the Supplier in accordance with the Call-Off Contract.

7.4 To enable performance of Maintenance and Support Services, the Buyer shall Support Services, the Buyer shall;

7.4.1 carry out Updates when reasonably requested;

7.4.2 comply with Supplier standards;

7.4.3 maintain configurations in accordance with Supplier guidance;

7.4.4 provide detailed error information; and

7.4.5 facilitate access to cloud environments as required.

7.5 Maintenance and Support Services shall not include issues arising from:

7.5.1 defects outside warranty;

7.5.2 Buyer failure to comply with responsibilities;

7.5.3 third-party platforms or integrations not approved by Supplier; or

7.5.4 changes in law.

7.6 Maintenance and Support Services shall not cover:

7.6.1 data restoration unless expressly agreed;

7.6.2 changes required due to legal or regulatory change, except mandatory safety requirements

7.7 Support and Maintenance Services shall be provided for the period specified in the Call-Off Contract. Beyond that period, the Supplier may terminate or charge additional fee

PART D – SUPPLIER LICENCE TERMS - GENERAL CLAUSES

1. DATA PROTECTION

1.1 The Parties agree that the terms of Appendix 2 of the Data Protection Agreement under Supplier Standard Terms shall apply to the extent that the Supplier acts as a Processor and processes Personal Data on the Buyer's behalf in the provision of the Services, and the Parties agree to comply with such terms. The Parties shall complete the details set out in Appendix 2 of the Data Protection Agreement in relation to the Processing of Personal Data by Supplier or a Third-Party Provider on a case-by-case basis. Notwithstanding the aforesaid, the Buyer acknowledges and agrees that the terms set out in the relevant Third-Party Provider's Third-Party Terms shall apply to the Processing of Personal Data by the Third-Party Provider acting as an independent controller or processor, as applicable.

1.2 Any breach by the Buyer of Data Protection Legislation and/or of any of the data protection provisions set out in the Call-Off Contract (including in the Supplier Terms) shall be deemed to be a Material Breach entitling the Supplier to end the Call-Off Contract.

1.3 The Buyer shall defend and harmless the Supplier, Supplier Staff and Supplier Processor Personnel against any and all Losses incurred if the Buyer, the CCS, any End User or any Buyer third-party breaches Joint Schedule 10 (Processing Data) of the Framework Contract, this Clause 1, any Data Protection Legislation or the Law, to the extent such breach is attributable to Buyer-controlled Processing or Buyer Elements.

1.4 The Buyer shall, and shall procure that its sub-processors, End Users, Associated Companies, sub-contractors, suppliers, agents and contractors comply with all its obligations under Data Protection Legislation when Processing Personal Data in connection with the Services. In this respect, the Buyer shall obtain and maintain all necessary registrations and authorisations with the competent data protection authorities and ensure it has and maintains a valid, lawful basis to Process Personal Data.

1.5 The Buyer shall notify the Supplier within a reasonable time of any changes to Data Protection Legislation or Law that may affect the contractual obligations of the Supplier under the Call-Off Contract and/or which may require a variation to be made to the data protection provisions, the technical and organisation measures, the Charges or the commercial terms. The Supplier may also submit proposals to the Buyer if the Supplier deems a certain change to be necessary to remain compliant with Data Protection Legislation or Law.

1.6 Each Party shall reasonably cooperate with the other in responding to data subject requests and regulatory enquiries, to the extent required by applicable law and to the extent such cooperation relates to Processing activities for which that Party is responsible.

1.7 Unless otherwise expressly agreed in the Call-Off Contract, Buyer Content and Personal Data may be processed and stored within the United Kingdom and/or the European Economic Area. The Supplier shall not be required to guarantee data residency beyond what is expressly stated in the Call-Off Contract, and any use of Third-Party Providers may be subject to their applicable data location arrangements, as notified to the Buyer.

2 LOSS OF BUYER CONTENT

2.1 The Supplier shall not be liable (whether in contract, tort (including negligence), breach of statutory duty, indemnity or otherwise) for any losses consequent upon the unauthorised access to, loss of, damage or destruction to, or corruption or degradation of any Buyer Content (including for the avoidance of doubt any systems or programs) nor the cost of reconstituting the same (whether such loss or damage was foreseeable, known or otherwise). any liability of the Supplier for loss or damage of any Buyer Content (including for the avoidance of doubt any systems or programs) which is not Buyer Data (whether the back-up is the responsibility of the Buyer or of the Supplier) shall be limited to the cost of reloading or restoring the last viable back-up copy (if any).

2.2 The Buyer agrees that, for the avoidance of doubt, its liability for all defaults by it resulting in direct loss, destruction, corruption, degradation or damage to any Supplier data (including any Supplier Personal Data), will not exceed the greater of the amounts set out in the Call-Off Contract for Buyer Data Defaults.

3 WARRANTIES AND INDEMNITIES

3.1 The Buyer undertakes, warrants and represents that:

3.1.1 it has full power and authority to enter into the Call-Off Contract, to apply for and maintain an Account and to access and/or use the Services;

3.1.2 all documentation, data and information (including Buyer Content) furnished to the Supplier by the Buyer or its representatives is current, complete, true, accurate and of appropriate quality for the Supplier's use in discharging its obligations under the Call-Off Contract. The Supplier shall be entitled to rely upon such documentation, data and/or information in performing the Services and shall not be liable for any errors in the accuracy or completeness thereof;

3.1.3 the Buyer Elements (including all data that the Buyer provides to the Supplier or any Supplier Party) have been checked by the Buyer and are free from any type of Malicious Software and virus;

3.1.4 the Buyer Elements and the Buyer's and/or any End User's access to and/or use of the Buyer Account or the Buyer Elements in connection with the Service Elements (or any part thereof) or their access to and/or use of the Service Elements (or any part thereof) themselves (including any connectivity to them) will not infringe applicable law or the intellectual property, privacy or other rights of the Supplier's, its lessors, any Supplier Party's, or any other third-party rights (including any Intellectual Property Rights);

3.1.5 the Supplier's or any Supplier Party's receipt of, access to and/or use of any item supplied directly or indirectly by the Buyer for use in connection with the provision of the Service Elements shall not cause the Supplier or any Supplier Party to infringe any third-party's rights (including any Intellectual Property Rights) in such item;

3.1.6 Buyer Content shall not contain any: (i) credit, debit or other payment card data; and/or (ii) data of national security or relating thereto;

3.1.7 the Buyer shall not access and/or use the Service Elements where a failure or fault of the Service Elements could lead to death or personal injury and in particular (by way of example and not limitation) the Service Elements should not be used for production services associated with mass transit systems, nuclear or chemical facilities, or medical support devices; and

3.1.8 the Buyer conducts its business in accordance with good ethical standards and in compliance with the processes required under the Bribery Act 2010 and any other analogous regulations or laws in any relevant jurisdiction.

3.1.9 the Buyer owns or otherwise has the right to use, and to entitle the Supplier to use in accordance with these Supplier Terms, all Buyer Content without infringing the intellectual property, privacy or other rights of any other person or entity.

3.2 The Buyer grants the Supplier a non-exclusive, royalty-free, worldwide licence for the Term of the Call-Off Contract to process, copy, display, transfer to third parties and otherwise use Buyer Content:

3.2.1 for the purpose of complying with the Supplier's obligations under these Supplier Terms and the Call-Off Contract; and

3.2.2 solely on an aggregated and anonymised basis for the purpose of improving the Supplier's products and offerings, or as otherwise agreed between the Parties.

The Supplier shall store and process Buyer Content in accordance with this DPA.

3.3 The Buyer is solely responsible for the accuracy, quality, integrity, legality, reliability and appropriateness of all Buyer Content. The Supplier assumes no responsibility for the lawfulness or quality of Buyer Content or the Buyer's use thereof. The Supplier reserves the right to withhold or delete any Buyer Content which is not in compliance with the Supplier Terms or its Acceptable Use Policy, subject to compliance with applicable law and, where reasonably practicable, prior notice to the Buyer.

3.4 The Supplier shall take reasonable actions to prevent the loss or alteration of Buyer Content within the Service Elements and up to the Service Boundary. However, unless otherwise expressly agreed in the Supplier Terms or in the Call-Off Contract, the Supplier shall not be responsible for any loss, alteration or inability to access or use Buyer Content. The Supplier recommends that the Buyer regularly create backup copies of all relevant data. The Buyer remains solely responsible for the availability and recovery of its data, including (without limitation) compliance with any tax or data retention obligations.

3.5 The Buyer shall assume all responsibility and liability in respect of its and its End Users' access to and/or use of the Service Elements. Accordingly, the Buyer will defend and hold harmless the Supplier, its lessors and all Supplier Parties for any and all claims, losses, damages, liabilities, costs and expenses (including reasonable legal fees) arising out of or in relation to any third-party claim arising from, including but not limited to,: (i) a breach of or non-compliance with any obligations or warranties under the Call-Off Contract; (ii) the Buyer Elements; (iii) any act or omission of the Buyer, any End User or any third party acting on the Buyer's or any End User's behalf or arising directly or indirectly from the Buyer's and/or any End Users possession, operation, access, use, modification or supply to a third party of anything provided under or otherwise out of or in connection with the Call-Off Contract; and (iv) any dispute arising between the Buyer and any End User. The Buyer acknowledges and agrees that the Buyer shall be responsible to implement necessary and sufficient protection measures for any Buyer Elements that the Buyer will use to access the Services and/or the Service Elements and that the Supplier shall have no responsibility for any Malicious Software, denial of service (DOS) and/or distributed denial of service (DDOS) attacks, bugs or similar item arising from Buyer-controlled configurations or Buyer Elements.

3.6 The Supplier shall deliver the Services by appropriately experienced, qualified and trained personnel and in a professional

manner with reasonable care, skill and diligence.

3.7 The Supplier will, so far as it is permitted, pass to the Buyer the benefit of any warranties in respect of any Third-Party Content, Third-Party Service and/or Third-Party Environment where such Third-Party Content, Third-Party Service and/or Third-Party Environment is provided by the Supplier to the Buyer as part of, in connection with or as a Service.

3.8 Save for any express warranties given hereunder, the Service Elements are provided on an 'as available' basis, except as expressly stated in the Call-Off Contract and, accordingly the Supplier, its lessors and each Supplier Party expressly disclaim any and all warranties of any kind or nature to the fullest extent permitted by law, whether express, implied, statutory or otherwise, relating to the Service Elements, including without limitation any warranties of title, non-infringement, merchantability, accuracy of informational content, satisfactory quality, fitness for a particular purpose or quiet enjoyment, together with any warranties arising out of any course of dealing, usage or trade.

3.9 The Supplier, its lessors and any Supplier Party make no representation or warranty regarding:

3.9.1 The results to be obtained from the Services or Service Elements;

3.9.2 whether the Services or Service Elements will meet the Buyer's or any End User's requirements;

3.9.3 whether the Services or Service Elements will be uninterrupted, timely, error-free, free from harmful; components, or that all errors can be corrected; or

3.9.4 whether any Content or Buyer Elements will be secure or free from loss or damage.

3.10 The Buyer acknowledges that:

3.10.1 there may be occasions when the Services (or any Service Elements) are unavailable or inaccessible; and

3.10.2 the Supplier shall not be liable for any loss or damage suffered by the Buyer or its users as a result of such unavailability, except to the extent expressly covered by Service Levels or service credits set out in the Call-Off Contract.

Although the Supplier will use commercially reasonable efforts to keep the Services free from viruses and protect against attacks, it does not guarantee that the Services will be virus-free and accepts no liability for damages resulting from attacks. The Buyer is responsible for implementing appropriate security measures and virus scanning before downloading any information, software or documentation, or otherwise using the Services.

4. TITLE, INTELLECTUAL PROPERTY RIGHTS AND INTELLECTUAL PROPERTY RIGHTS INDEMNITY

TITLE AND INTELLECTUAL PROPERTY RIGHTS

4.1 Nothing in the Call-Off Contract shall affect the Buyer's Intellectual Property Rights in any data, information, software, materials or other content provided or made available by or on behalf of the Buyer or its End Users in connection with the Services (including any Buyer Content). The Buyer hereby grants (or shall procure the grant of) to the Supplier a non-exclusive, royalty-free, worldwide licence for the Term of the Call-Off Contract to host, process, transmit, display, copy and otherwise use the Buyer Content and Buyer Elements solely to the extent necessary for the provision, operation and support of the Services in accordance with the Call-Off Contract, applicable law and the Supplier's documented instructions. Except as expressly set out in this Clause 4.1, the Supplier shall not acquire any right, title or interest in or to the Buyer Content or Buyer Elements.

4.2 All Intellectual Property Rights of whatever nature in the Service Elements and all other materials supplied or developed under the Call-Off Contract in whatever form including any hardware, software, firmware and documentation are and shall remain vested in the Supplier and/or its licensors. Nothing in the Call-Off Contract shall operate to assign, transfer or otherwise convey to the Buyer any Intellectual Property Rights in the Service Elements, except for the limited rights expressly granted to the Buyer to access and use the Services during the Term.

4.3 The Buyer agrees that:

4.3.1 any licence granted by the Supplier to the Buyer to "use" the Supplier Background IPRs embedded in the Project Specific IPRs shall mean to use the Supplier Background IPRs solely as part of the Project Specific IPRs and the Buyer shall not disclose, provide access to, sub-licence, disassemble, decompile, reverse engineer, modify, transfer or assign any Supplier Background IPRs to an Associated Company or any other third party without the Supplier's prior written consent, save to the extent such restriction would prevent the Buyer from using Buyer Elements deployed on the Services in accordance with the Call-Off Contract;;

4.3.2 the Supplier may use Open Source Software or code in the provision of any of the Services (including in any Service Element);

4.3.3 the Supplier shall not be obligated to provide the source code or object code version of the Supplier Background IPRs used for the provision of Services. The Buyer agrees that, save as set out in the Call-Off Contract and these Supplier Terms, neither the Buyer nor any of its employees, suppliers, vendors, or any other third party shall use or

have access to any Supplier Background IPRs used to provide the Services; and

4.3.4 upon completion of the Services, the Supplier shall have the right to withdraw the Supplier Background IPRs which are not embedded within Project Specific IPRs from the Buyer's environment, provided that such withdrawal shall not prevent the Buyer from accessing or exporting Buyer Content or Buyer Elements in accordance with the exit provisions of the Call-Off Contract.

4.4 In accordance with the Call-Off Contract, if the Supplier informs the Buyer that it is not able to comply with Call-Off Schedule 1 (Intellectual Property Rights) of the Call-Off Contract and:

4.4.1 the Buyer and the Supplier shall work together to agree licence terms acceptable to the Buyer (acting reasonably) at the time;

a. in the absence of an agreement by the parties, the parties agree that the default licence position in relation to any IPRs, the IPR Option A4 under Call-Off Schedule 1 (Intellectual Property Rights) shall apply.

b. and the Buyer agrees that such licence terms are acceptable to it.

4.5 The Buyer shall ensure that all End Users comply with:

4.5.1 the terms of the Call-Off Contract;

4.5.2 these Supplier Terms;

4.5.3 any Acceptable Use Policies or security requirements notified by the Supplier from time to time; and

4.5.4 all applicable third-party licence terms relating to the Services, which have been identified and set out in the Order Form of the Call-Off Contract.

4.6 The Buyer shall remain responsible for all acts and omissions of its End Users in connection with the use of the Services.

5 INTELLECTUAL PROPERTY RIGHTS INDEMNITY

5.1 The Supplier shall have no liability to the extent that an IPR Claim arises out of or relates to:

5.1.1 any access to or use of the Services by the Buyer or any End User in excess of the scope of the licence granted, or otherwise in breach of the Call-Off Contract or any applicable licence terms;

5.1.2 the access, use or combination of the Services or any Service Elements with any third-party software, hardware, data, systems or services not supplied by, or not expressly permitted by, the Supplier in the Service documentation or service descriptions, where such access, use or combination gives rise to the IPR Claim;

5.1.3 any access to or use of the Services or Service Elements otherwise than in accordance with the Call-Off Contract, the Supplier's published documentation or the Supplier's reasonable written instructions, or for a purpose for which the Services were not designed or intended;

5.1.4 any modification, alteration or adaptation of the Services or Service Elements made by any person other than the Supplier or its authorised representatives;

5.1.5 any configuration, specification or modification of the Services implemented by the Supplier solely to the extent required by the Buyer's specific written instructions, where such instructions directly give rise to the IPR Claim;

5.1.6 the Buyer's continued use of an older, superseded or unsupported version of the Services or Service Elements where the Supplier has made available a newer version that would have avoided the alleged infringement; the Buyer's refusal or failure, following reasonable notice from the Supplier, to:

a. permit the Supplier to modify the Services so as to avoid the alleged infringement;

b. accept a functionally equivalent substitute service; or

c. accept reasonable and customary third-party licence terms relevant to the IPR Claim; or

d. any access, use or combination of the Services or Service Elements with any Buyer Content or other materials not supplied by the Supplier, to the extent that such access, use or combination directly causes the IPR Claim.

5.2 In relation to any IPR Claim for which the Buyer seeks indemnification under the Call-Off Contract, the Buyer shall:

5.2.1 notify the Supplier promptly upon becoming aware of any claim, notice or threat of an IPR Claim;

5.2.2 not make any admission, agreement or compromise relating to the IPR Claim without the Supplier's prior written consent;

5.2.3 grant the Supplier sole control of the defence and settlement of the IPR Claim, provided that the Supplier shall not settle any IPR Claim in a manner that imposes any material obligation on the Buyer without the Buyer's prior written consent (not to be unreasonably withheld or delayed);

5.2.4 take reasonable steps to mitigate any loss or damage arising from the IPR Claim;

5.2.5 provide the Supplier with such reasonable assistance and information as the Supplier may request in connection with the defence of the IPR Claim; and

5.2.6 not unreasonably withhold or delay any approval required to enable the Supplier to implement a workaround, modification or substitute service.

Failure by the Buyer to comply with this Clause 5.2 shall relieve the Supplier of its obligations under Clauses 4.2 and 4.3 only to the extent that such failure materially prejudices the Supplier's ability to defend or settle the relevant IPR Claim.

5.3 Subject to any rights or remedies which cannot be excluded or limited as a matter of applicable law or are expressly

preserved under the Call-Off Contract, the indemnities set out in the Call-Off Contract shall constitute the Buyer's sole and exclusive remedy, and the Supplier's entire liability, in respect of any actual or alleged infringement of any Intellectual Property Rights arising from or in connection with the Services.

SUSPENSION

6.1 The Supplier may, acting reasonably and proportionately, suspend any right to access and/or use the Service Elements, the Buyer Account or the Buyer Elements (within its control) or any part thereof (whether by the Buyer and/or any End User or any third party acting on their behalf) only to the extent necessary and immediately where required, without notice to the Buyer if the Supplier determines, acting reasonably, that:

6.1.1 the access to and/or use of the Service Elements, the Buyer Account and/or the Buyer Elements (within its control) or any part thereof:

a. poses a security risk (including any security risk to third parties);

b. may have an adverse impact upon the Service Elements, the Buyer Account and/or the Buyer Elements or any part thereof;

c. may have an adverse impact upon the relevant systems;

d. may have an adverse impact on any other Supplier customer and/or end user; or

e. may subject the Supplier, its lessors, any Supplier Party or any third party to any liability;

6.1.2 the Buyer, or any End User, is in material breach of the Call-Off Contract (including where the Buyer fails to make payment of any undisputed Charges upon the date that payment is due (including any Charges that are deemed to be undisputed), and such breach has not been remedied within a reasonable period following written notice, except where immediate suspension is required to comply with law or to mitigate risk;

6.1.3 there is or has been any attack on the system, notably via a virus, which may alter the capacity, the integrity and/or the security of the Service Elements, the Buyer Account and/or the Buyer Elements or any part thereof; or

6.1.4 suspension or restricted access to the Service Elements, the Buyer Account and/or the Buyer Elements (within its control) or any part thereof is requested by a judicial or administrative authority.

6.2 Where reasonably practicable, and consistent with Framework Contract continuity principles, the Supplier shall provide advance notice of suspension and shall take reasonable steps to minimise the impact of any suspension on the Buyer's use of the Services.

6.3 The Supplier may suspend any right to access and/or use the Service Elements, the Buyer Account or the Buyer Elements (within its control) or any part thereof (whether by the Buyer and/or any End User or any third party acting on their behalf) immediately without notice to the Buyer only in any circumstances in which the Supplier is otherwise entitled to terminate the Call-Off Contract and where suspension is necessary as an interim protective measure.

6.4 If the Supplier suspends the Buyer's and/or any End User's access to or use of the Service Elements, the Buyer Account and/or the Buyer Elements (within its control) or any part thereof:

6.4.1 other than for Buyer and/or End User default:

a. the Buyer shall remain liable for all amounts payable up to and including the date of suspension; and

b. the Buyer shall remain liable for all amounts payable for any Services to which the Buyer and/or any End User continue to have access and/or use of during the period of suspension.

6.4.2 for Buyer and/or End User default, the Buyer shall remain liable for all amounts payable for all Services provided, including any Services suspended by the Supplier in accordance with this clause.

Nothing in this Clause 6.4 shall prevent the Buyer from accessing or exporting Buyer Content or Buyer Elements during a suspension, to the extent required to meet legal, regulatory or public service continuity obligations, unless prohibited by law or required for security reasons.

6.5 The Supplier may, acting reasonably and proportionately, lift a suspension (or part thereof) at any time. The Buyer shall be responsible for all Charges payable for the Services provided after the date that the suspension has been lifted and, where the suspension is as a result of a Buyer and/or End User default, the Buyer shall, in addition, be liable for the Re-Activation Charge.

6.6 The Supplier's right to suspend the Buyer's and/or any End User's right to access and/or use the Service Elements, the Buyer Account and/or the Buyer Elements (within its control) or any part thereof is in addition to any other right the Supplier may have under the Call-Off Contract, at law or otherwise, subject always to compliance with the Framework Contract and relating to proportionality, transparency and continuity of service.

7 CHARGES AND PAYMENT

7.1 All Charges are exclusive of Taxes and expenses which shall, in addition, be payable by the Buyer. Any Taxes due shall be charged at the rate prevailing at the date of the invoice. Expenses shall, unless otherwise agreed in the Call-Off Contract or set out in the Charges description relating to the Service, be charged at cost.

7.2 Unless otherwise provided for in the Call-Off Contract or set out in the Charges description relating to the Service, all expenses, fees and other amounts shall be invoiced monthly in arrears.

7.3 If the Buyer disputes any amounts in any invoice submitted by the Supplier, it shall follow the procedure set out in the Call-Off Contract. In the event that the Buyer does not advise the Supplier of any disputes within ten (10) Working Days of the receipt of the invoice, the invoice shall be deemed to have been accepted without dispute and the Buyer shall pay the same forthwith together with any interest to which the Supplier is entitled under the Call-Off Contract.

7.4 Subject to the Framework Contract remaining in force, the Charges shall be increased with effect from the date immediately following the expiry of the initial period of the Call-Off Contract and on each subsequent anniversary during the Term as follows:

7.4.1 for those Services performed inside the United Kingdom, by a percentage equal to the percentage increase in the Index for the twelve months ending sixty days prior to the relevant adjustment date, together with any additional percentage mark-up agreed by the Parties in writing, subject always to compliance with the Framework Contract and any applicable CCS approval requirements; and

7.4.2 for Services performed outside the United Kingdom, by a percentage equal to the increase in the Relevant Indexation Rate for the twelve (12) months ending sixty (60) days prior to the relevant adjustment date, together with any additional percentage mark-up agreed by the Parties in writing, subject always to compliance with the Framework Contract and any applicable CCS approval requirements.

7.5 Unless specifically agreed by the Supplier in the Call-Of Contract, any discount pricing offered by the Supplier shall not apply to any Third-Party Elements, including third-party cloud infrastructure, platform services or software licences that are charged on a pass-through or consumption basis.

8 RELIEF EVENTS/ BUYER DEPENDENCIES

8.1 The Supplier shall not be in breach of its obligations nor incur any liability whatsoever to the Buyer or any End User where it is prevented and/or delayed from complying with and/or performing any of its obligations under the Call-Off Contract to the extent caused by reason of:

8.1.1 any act, omission or default of the Buyer, any End User or any third party acting on behalf of the Buyer or any End User;

8.1.2 any delay or failure by the Buyer or any End User or any third party acting on behalf of the Buyer or any End User to comply with any of its obligations as set out in the Call-Off Contract; or

8.1.3 the non-fulfilment of any assumptions or dependencies (including any Buyer Responsibilities)set out in the Call-Off Contract or the Service Definition.

Accordingly, the Supplier shall have the right to an extension of time to perform its obligations by such reasonable period having regard to the nature and duration of such prevention and/or delay. The Supplier shall also have the right to be paid all reasonable and demonstrable costs, charges and losses sustained or incurred by the Supplier directly as a result thereof, and any part of the Charges which would, but for such act, omission, default or non-fulfilment, have been payable pursuant to the Call-Off Contract,

9 LIMITATION OF LIABILITY

9.1 The Buyer's liability to pay the Supplier in accordance with the Call-Off Contract shall not be limited by this Clause 9.

9.2 In no event shall the Supplier be liable for the following types of loss:

9.2.1 any and all direct or indirect:

9.2.2 loss of contracts;

9.2.3 loss of use of the Buyer Elements or the Buyer Environment;

9.2.4 financing expenses;

9.2.5 losses arising from interruption in the use or availability of data; or

9.2.6 losses arising from stoppage to other work; or

9.2.7 any loss or damage that could have been avoided had the Buyer kept full and up-to-date back-up and security copies of any software or data held or used by or on behalf of the Buyer.

9.3 The Supplier shall not be liable for the fraudulent or unauthorised use of the Subscription Services by the Buyer and/or any third party. For the avoidance of doubt, the Buyer shall be obliged to pay Charges for all use of the Subscription Software,

whether or not such use results from unauthorised access or use by third parties. The Supplier shall also not be liable for any loss, costs, expenses and/or damages arising from or in connection with a Network Operator denying or withdrawing any connection facilities.

9.4 The Buyer will be liable for the following types of loss, which shall be regarded as direct and recoverable by the Supplier:
- 9.4.1 any regulatory losses or fines arising directly from the Buyer's breach of any Laws;
- 9.4.2 any additional operational or administrative costs and expenses arising from any material breach by the Buyer;
- 9.4.3 any wasted expenditure or unnecessary costs and expenses incurred by the Supplier as a result of any act or omission, default or misuse by the Buyer, any Buyer third party or any End User; and
- 9.4.4 any other liabilities suffered by the Supplier in connection with the loss of, corruption of, or damage to any Service Elements.

9.5 The Parties agree that the exclusions and limitations of liability set out in the Call-Off Contract shall exclude and limit the Supplier's liability to the Buyer in respect of all matters arising out of or in connection with the Call-Off Contract, whether in contract, tort (including negligence), breach of statutory duty, indemnity or otherwise.

9.6 Save in respect of any liability for death or personal injury resulting from negligence, the Buyer shall not bring any claim in contract, tort (including negligence), breach of statutory duty, indemnity or otherwise against the Supplier or any Supplier Associated Company, or their respective officers, directors, employees or agents, in respect of any matter arising out of or in connection with the Call-Off Contract. The Buyer agrees that no such person owes the Buyer a duty of care in respect of such matters. The Parties agree that the benefit of this Clause 9.6 shall be enforceable by the Supplier, each Associated Company and their respective officers, directors, employees or agents in accordance with the Contracts (Rights of Third Parties) Act 1999 or any other applicable law.

9.7 Nothing in the Call-Off Contract excludes or limits liability for fraud, fraudulent misrepresentation, or death or personal injury caused by negligence.

9.8 Nothing in these Supplier Terms shall limit or exclude liability to the extent that such limitation or exclusion is prohibited by the Framework Contract or the Call-Off Contract.

10 AUDIT

10.1 The Supplier (or any third party appointed by the Supplier) may on reasonable notice and during normal business hours audit the Buyer's and/or any End User's compliance with the terms of the Call-Off Contract, to the extent relevant to the Buyer's use of the Services. The Buyer shall (and shall procure that all End Users shall):
- 10.1.1 cooperate with the Supplier (and any third party appointed by the Supplier) with respect to the audit; and
- 10.1.2 provide all reasonable assistance and access to information, records and systems under the Buyer's control that the Supplier may reasonably request solely for the purpose of verifying compliance with these Supplier Terms.

10.2 The Supplier shall use its reasonable endeavours to ensure that any such audit does not unreasonably interfere with the Buyer's normal business operations or the continuity of public services. Any information obtained by the Supplier or its auditors in connection with an audit shall be used solely for the purpose of verifying compliance with the Call-Off Contract and enforcing the Supplier's rights thereunder and shall not be disclosed to any third party except as required by law or regulatory authority.

10.3 Where an audit determines that:
- 10.3.1 the Buyer and/or any End User is accessing and/or using the Service Elements (or any part thereof) in excess of its rights under the Call-Off Contract, the Buyer agrees to pay within thirty (30) days of written notification from the Supplier any charges or fees applicable to its access and/or use of the Service Elements (or any part thereof) in excess of its rights under the Call-Off Contract;
- 10.3.2 the Buyer and/or any End User is in breach of any warranty or obligation under the Call-Off Contract, the Buyer shall, if such breach can be remedied, remedy or, procure the remedy, of such breach within thirty (30) calendar days of receiving written notification from Supplier requiring it to be remedied.

10.4 If the Buyer does not pay the charges and fees due under the Call-Off Contract or remedy the breach the Supplier may:
- 10.4.1 suspend any right to access and/or use the Service Elements, the Buyer Account or the Buyer Elements or any part thereof (whether by the Buyer and/or any End User); and/or
- 10.4.2 terminate the Call-Off Contract,

immediately on notice to the Buyer without incurring any penalty or liability to the Buyer or any End User.

10.5 The Buyer agrees that the Supplier shall not be responsible for any costs the Buyer or any End User may incur in relation

to an audit. All the Supplier's costs in relation to an audit shall be borne by the Supplier, save for where Clauses 10.3 or 10.4 apply and a material breach or material overuse is identified, in which case the Buyer will reimburse the Supplier for all costs and expenses in relation to such audit on first demand. Where an audit does not identify a material breach or material overuse of the Services, the Supplier shall not conduct a further audit of the same Buyer for a period of three (3) months, unless required to do so by law or a regulatory authority.

11 TERM, TERMINATION, CONSEQUENCES OF TERMINATION AND EXIT

TERM

11.1 These Supplier Terms shall take effect on the effective date of the relevant Call-Off Contract and shall remain in force until terminated by either Party in accordance with these Supplier Terms or the termination provisions set out in the Call-Off Contract.

TERMINATION

11.2 Either Party may terminate the Services in accordance with the terms in the Call-Off Contract.

11.3 Without prejudice to any other right of termination the Supplier may have under the Call-Off Contract, at law or otherwise, the Supplier may terminate the Services immediately by written notice to the Buyer without incurring liability for such termination if:

11.3.1 any misuse, act or omission by the Buyer, an End User or any third party acting on the Buyer's or an End User's behalf results in the suspension of any right to access and/or use the Service Elements, the Buyer Account, the Buyer Elements and/or any part thereof for a period of more than thirty (30) days, save in relation to the failure by the Buyer to pay any undisputed Charges, where the Supplier shall be entitled to terminate the Call-Off Contract;

11.3.2 acting reasonably, it considers that the activities the Buyer and/or any End User are engaged in might be materially detrimental to the Supplier's or any Supplier Party's reputation; or

11.3.3 the relationship of the Supplier with a third party which provides software or other technology or service that the Supplier depends on to provide the Services expires, terminates or requires the Supplier to change the way it provides such software or other technology or service as part of the Services or prohibits the Supplier from selling such software or other technology or service as part of the Services and the Supplier is unable, acting reasonably, to replace such software, technology or service with a similar software, technology or service at the same commercial rates; or

11.3.4 it reasonably suspects that there might be fraudulent or illegal activity in connection with the Buyer's access and/or use of the Service Elements (or any part thereof); or

11.3.5 the Supplier is required to do so in order to comply with an applicable Law (including any national or international foreign trade or customs requirements or any embargoes or other sanctions) or order or direction of any regulatory authority of competent jurisdiction.

11.4 Additionally, the Supplier may terminate the Services for convenience on not less than thirty (30) days' written notice, provided that such termination right shall apply only to the extent permitted under the Framework Contract and Call-Off Contract.

CONSEQUENCES OF TERMINATION

11.5 Upon the expiry or termination for any reason of the Call-Off Contract:

11.5.1 all the Buyer's and any End User's rights and permissions under the Call-Off Contract (including any Third-Party Terms) shall immediately terminate;

11.5.2 the Buyer shall, and shall procure that all End Users shall, immediately cease to use the usernames, passwords and other sensitive information, and for the avoidance of doubt, the Buyer shall, and shall procure that all End Users shall, immediately cease to access and/or use the Services and the Buyer Account;

11.5.3 the Buyer will immediately deliver up or, if directed by the Supplier, destroy, all Confidential Information, Supplier Content and Third-Party Content, and all copies of the same, in the Buyer's possession, custody or control and shall at the Supplier's request certify in writing to the Supplier that the same has been done;

11.5.4 where applicable and subject to prior notice, the Supplier shall be entitled to enter upon Buyer premises for the purposes of recovering any equipment or materials (including work-in-progress) which are the Supplier's or a Supplier Party's property, for which purpose the Buyer hereby grants the Supplier an irrevocable licence to enter such premises; and

11.5.5 the Buyer shall pay the Supplier all sums due under the Call-Off Contract up to the date of termination or expiry.

11.6 The Supplier shall be entitled to take such actions as it considers necessary to delete Buyer Content from the Services on

instruction from the Buyer or no earlier than twelve (12) calendar months from the expiry or termination of the Call-Off Contract (whichever is the earlier) without incurring liability to the Buyer, any End User or any third party. During the said period, subject to the Buyer having paid all outstanding amounts due under the Call-Off Contract (including any Charges for use of the Services following such termination), the Supplier shall provide the Buyer with access to the Buyer Content so that the Buyer may remove or delete Buyer Content from the Services.

11.7 For the purposes of the Call-Off Contract, references to "data (including Buyer Data)" shall be limited to data belonging to the Buyer and shall not include any Supplier Content, Service Elements, operational data, metadata, system logs or any Third-Party Content.

EXIT

11.8 Exit assistance shall be provided in accordance with the Call-Off Contract, and any charges for such exit assistance shall be limited to the Supplier's reasonable, pre-agreed time and materials rates.

11.9 Upon expiry or termination of the Call-Off Contract for any reason, the Buyer shall be responsible for extracting Buyer Content using the standard tools, interfaces and functionality made available by the Supplier as part of the Services. The Supplier shall not be responsible for any failure by the Buyer to extract Buyer Content prior to its deletion in accordance with the Call-Off Contract.

11.10 If compliance with any exit-related obligation would cause the Supplier to breach any applicable law (including Data Protection Legislation) or to perform any unlawful act, the Supplier shall comply with such obligation only to the extent that it is reasonably practicable to do so without breaching applicable law, including, where appropriate, by providing information in an anonymised or aggregated form.

11.11 For the avoidance of doubt, the Parties agree that the provision of the Services does not involve the assignment of dedicated personnel to the Buyer and is not intended to constitute a relevant transfer for the purposes of the Transfer of Undertakings (Protection of Employment) Regulations 2006 or any similar legislation.

12 IMPORT/EXPORT

12.1 Each Party shall comply with all applicable export control laws, trade restrictions and economic sanctions regulations in connection with its performance under these Supplier Terms, including those of the United Kingdom, the European Union, and the United States.

12.2 The Buyer agrees that it shall not, and shall ensure that its End Users do not, use the Services in or in relation to any activities involving:

12.2.1 any country subject to comprehensive economic sanctions under UK, EU or US law (including, without limitation, Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine);

12.2.2 any party in breach of applicable trade control laws; or

12.2.3 any activities requiring government authorisation, without first obtaining the written consent of the Supplier and any required authorisations.

12.3 For the avoidance of doubt, the Buyer shall not grant access to the Services to any individual, entity or organisation that is subject to trade sanctions or embargoes under UK, EU or US law, or that appears on the UK Sanctions List, the EU Consolidated Sanctions List, or the OFAC Specially Designated Nationals List from time to time.

13 FORCE MAJEURE

13.1 Without prejudice to the definition of Force Majeure set out in the Call-Off Contract, the parties agree that such definition shall, in addition, also include:

13.1.1 acts of God, flood, drought, earthquake, hurricane, volcanic eruption or other natural disaster;

13.1.2 epidemics and pandemics (including communicable disease outbreaks and public health emergencies) whether identified, declared or accepted as such under the relevant laws and/or regulations or not;

13.1.3 terrorist attack, civil war, civil commotion, civil unrest, civil protests, riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo or breaking off of diplomatic relations;

13.1.4 breakdown of law and order for a period exceeding 48 hours where the normal business activities cannot be carried on;

13.1.5 nuclear, chemical or biological contamination or sonic boom;

13.1.6 any law or any action taken by a government or public authority, including without limitation imposing an export or import restriction, quota or prohibition;

13.1.7 interruption or failure of utility service; and

13.1.8 death, illness or incapacity or any other form of unavailability of key personnel, provided that the affected party has made reasonable efforts to find a replacement and a period of seven (7) days has passed since the said efforts have started and no replacement has happened.

13.2 Both parties will use all reasonable endeavours to mitigate the effect of the Force Majeure event on the performance of their obligations. In particular, the parties will cooperate in good faith to adopt together some mitigation measures in order to decrease the impact of the Force Majeure event, such as remote working, off or nearshoring, etc, as far as they are proportionate, adequate and in compliance with the Law.

13.3 Subject to the Call-Off Contract, in the event of a Force Majeure, the time for performance shall be extended by a period equivalent to the period during which performance of the obligation has been delayed or failed to be perform.

14 SUBCONTRACTING AND CLOUD PROVIDERS

14.1 The Supplier may subcontract the provision of all or part of the Services to Supplier Parties, including hyperscale cloud providers, provided that the Supplier remains responsible for its obligations under the Call-Off Contract.

15 THIRD PARTY ELEMENTS AND OPEN SOURCE SOFTWARE

15.1 The services, content and equipment used to provide the Services as set out in the Call-Off Contract may include Third-Party Elements supplied by a Third-Party Provider.

15.2 The use of those Third-Party Elements is subject to the terms and conditions of the applicable "Third-Party Terms", solely to the extent incorporated by reference in the Order Form, but only as if the Supplier (or, where the Third-Party Terms require a direct contractual relationship, the Third-Party Provider) and the Buyer were the parties to them. The Buyer acknowledges and agrees that the Third-Party Elements are provided on a pass-through basis and that the Supplier does not provide, and expressly disclaims, any warranties, guarantees or remedies in respect of the Third-Party Elements other than those expressly provided by the relevant Third-Party Provider under the applicable Third-Party Terms, which have been expressly set out in or referred to (by way of hyperlink or otherwise) in the Order Form.

15.3 The Buyer shall accept (and shall procure that End Users accept) any Third-Party Terms expressly identified in the Order Form as a condition of access to and use of the relevant Third-Party Elements, including where such acceptance is required through click-through, online or similar mechanisms implemented by the Third-Party Provider.

15.4 In the event of any conflict between the Third-Party Terms and the Call-Off Contract, the Third-Party Terms shall prevail solely in respect of the Third-Party Elements and to the extent of such conflict.

15.5 The use of Third-Party Elements is subject to the Buyer (including all its End Users) complying with the obligations and requirements applicable to users of those Third-Party Elements as set out in the relevant Third-Party Terms. Insofar as the Buyer has any obligations under the Third-Party Terms, it shall procure that its Associated Companies, End Users and any third parties acting on its or their behalf comply with those obligations, and the Supplier shall have no liability arising from any breach of the Third-Party Terms by the Buyer or any End User.

15.6 The Buyer agrees that certain provisions of the Call-Off Contract expressly identified by the Supplier in the Order Form may not apply to the Third-Party Provider, or not be required to be flowed down by the Supplier in its agreements with the Third-Party Provider in relation to the Third-Party Elements, including where such provisions are inconsistent with, or not supported by, the Third-Party Provider's standard commercial terms or operating model.

15.7 Notwithstanding any other provision of the Call-Off Contract, the Third-Party Provider's data processing addendum and/or data protection terms expressly incorporated into the Call-Off Contract via the Order Form shall apply where the UK GDPR and/or EU GDPR applies to the Buyer's use of the Third-Party Elements to process Buyer Personal Data and/or Service Personal Data. Such data protection terms shall apply only to the extent they do not conflict with the Joint Schedule 10 Processing Data of the Framework Contract, and the Buyer acknowledges that the Supplier's obligations are limited to those capable of being passed through to the Third-Party Provider.

15.8 The Buyer shall provide sufficient notice to, and obtain all necessary consents and authorisations from, End Users and any other party providing Personal Data to permit the Processing of such data by the Third-Party Provider in accordance with the Call-Off Contract and the applicable Third-Party Terms as incorporated, and shall be solely responsible for any failure to obtain such consents or authorisations.

15.9 The Supplier shall communicate to or notify the Buyer in writing of any updates or amendments to any hyperlink referenced

in the Order Form or the Call-Off Contract, and any such updates or amendments shall apply automatically to the Third-Party Elements from the date specified by the relevant Third-Party Provider.

15.10 Where the Services and/or Service Elements include Open Source Software, the Buyer shall use such Open Source Software in accordance with the applicable open source software licence terms. Information regarding the relevant Open Source Software and applicable licence terms shall be communicated and/or provided to the Buyer by the Supplier. The applicable open source software licence terms shall prevail over the Call-Off Contract solely in respect of the relevant Open Source Software components.

16 CHANGE IN LAW

16.1 For the avoidance of doubt, the Buyer agrees that although the Supplier may not increase the Charges prices as a result of a general change in Law or a Specific Change in Law, without prior written approval from CCS, the Supplier will be entitled to charge the Buyer for any additional costs, losses and expenses (whether direct or indirect) incurred as a result of a general change in Law or a Specific Change in Law on a times and materials basis at the Supplier's rates set out in the Framework Contract or the Call-Off Contract (as the case may be).

PART E – SUPPLIER LICENCE TERMS - DEFINITIONS

1.1 In these Supplier Terms, unless the context requires otherwise or the terms are separately defined, the following terms shall have the following meanings:

"**Acceptance Period**"	shall have the meaning ascribed to it in Clause 4 of Part C - Cloud Support Services of the Supplier Licence Terms where Acceptance applies to the relevant Services;
"Acceptance Tests"	means the tests designed to check that the applicable Deliverables or Services, where Acceptance applies comply in all material respects with the Specification;
"Acceptance Test Criteria"	means the basis upon which the Acceptance Tests will be designed to check that the applicable Deliverables or Services, where Acceptance applies, comply in all material respects with the Specification;
"**Account**"	means the account created by the Supplier for use by the Buyer in connection with the Services;
"**Application Programming Interface**" or "**API**"	means a language and message format used by an application program to communicate with the operating system or some other control program, such as a database management system (DBMS) or communications protocol;
"**Associated Company**"	means any entity Controlled by or under the same Control as or Controlling the relevant Party, where "**Control**" means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "**Controls**", "**Controlled**" and "**Controlling**" shall be interpreted accordingly;
"**Background IPR**"	means any pre-existing works created by or on behalf of either Party (a) prior to the later of (i) the Effective Date of the Framework Contract or (ii) the effective date of the relevant underlying Call-Off Contract or other such implementation agreement under the Supplier Terms or (b) independently from the Framework Contract.
"**BCR**"	means the Binding Corporate Rules of the Supplier Group;
"**Buyer Content**"	means the Content that the Buyer or any End User: (i) runs on, accesses through or configures using the Services; (ii) causes to interface with the Services (including any Content necessary for connectivity or compatibility); (iii) uploads to, generates through, or stores within the Services; or (iv) otherwise provides, transmits, processes, uses or stores under or in connection with the Buyer Account, the Services or the Call-Off Contract. For the avoidance of doubt, Buyer Content includes Buyer Data, Buyer Personal Data and Buyer Software.
"**Buyer Elements**"	means the Buyer Content and the Buyer Environment;
"Buyer Environment"	means: (i) the hardware and other equipment, communications and other IT infrastructure at the Buyer premises; and (ii) the hardware and other equipment, communications and other IT infrastructure to which any Service Elements are required to connect and/or with which any Service Elements are required to operate, excluding the Supplier Environment and the Third-Party Environment;
"**Content**"	means, without restriction, software in all forms, code, command line tools, software libraries, web service definition language, documentation, data (including any Personal Data), text, audio, video, images, know-how, technologies, methodologies, processes, tools, working papers, or any other content;
"**Controlled Data**"	means any technical data such as blueprints, source code, drawings, plans, specifications, manuals or instructions which are required for the development, production or use of export-controlled products or software;
"**Devices**"	means the devices specified by the Supplier as being able to be used with the specific Service;
"**End User**"	means the Buyer and any individual authorised by the Buyer to access or use the Services;
"**General SLA Terms**"	means the general service level agreement terms and conditions relating to the Services set out in Section 1 of Supplier Service Specific Terms ;
"IaaS"	means the Infrastructure as a Service and any associated online services provided to the Buyer and specified in the Call-Off Contract;
"**Incident**"	means any event which is not part of the standard operation of the Service as set out in the Service Definition and which causes, or may cause, an interruption to, or a reduction in the quality of that Service, save in relation to SaaS where "**Incident**" shall have the meaning set out therein;

"**Index**"	means whichever of the indexes set out below with the greatest increase during the relevant period: (i) the annual index of salary increases published by Computer Economics Limited to participants in its Computer Staff Salary Survey; (ii) the Index of Retail Prices published by the Office for National Statistics (or the Government department upon which duties in connection with such index be devolved); or (iii) the Consumer Price Index (in the Central Statistical Office publication "Monthly Digest of Statistics"). Should any of these no-longer be published, they shall be replaced with such other appropriate index as the parties may agree at the time acting reasonably.
"Cloud Support Services Deliverables"	means where applicable an item or items of work expressly identified in the Call-Off Contract as deliverables provided as part of Cloud Support Services;
"**Location**"	means any location where the Supplier or a Supplier Party have premises from which Services are provided;
"Maintenance and Support Services"	shall mean the maintenance and/or support services provided by the Supplier to any Product (including Hardware and/or Software) as specified and agreed in the Call-Off Contract and/or the Call-Off Contract;
"Minor Defect"	means any error or defect which does not materially interfere with the effective use of the relevant Service, or which is cosmetic in nature;
"**New Functionality**"	means a new feature incorporated in an Upgrade or a New Version which is not available in the version licensed to the Buyer under the Supplier Terms;
"**New Version**"	means a set of systems software or applications software which the Supplier designates as a new version to the version licensed to the Buyer under the Supplier Terms and in which substantial new, but successor functionalities or other substantial changes (e.g. architectural) are introduced;
"Non-Conformity"	means a failure of part or all of a Service or Deliverable, where applicable to conform in any material respect with the Specification;
"Open Source Software" or "OSS"	means software (whether contained within the Subscription Software or otherwise) where the source code is available to the general public for use and modification, generally free of charge and, in each case, where customers are granted a right to use such open source software via an open source licence.
"PaaS"	means the platform-as-a-service and any associated online services provided to the Buyer and specified in the Call-Off Contract;
"**Re-Activation Charge**"	means the amount of all reasonable costs, charges and losses sustained or incurred by the Supplier or any Supplier Party as a result of the suspension and the reactivation of the Service Elements, the Buyer Account and/or the Buyer Elements or any part thereof;
"**Relevant Indexation Rate**"	means, for Services performed outside the United Kingdom, the relevant consumer price indexation rate in the country in which such Services are performed as agreed by the parties at the time;
"**Relevant Staff**"	means any personnel employed by the Supplier wholly or mainly in connection with the provision of the Services;
"**Resolution**" or "**Resolve**"	means that the normal operation of the Services has been restored and the Incident status has been set to resolved by the Supplier;
"**Resolution Time**"	means the time taken between the Supplier's confirmation of an incident being logged as an Incident and it being Resolved;
"**SaaS**"	means the software-as-a-service and any associated online services provided to the Buyer and specified in the Call-Off Contract;
"**Service Boundary**"	means the logical demarcation point between the Supplier-managed Service Elements and the Buyer-managed Buyer Elements, as described in the Service Definition or Call-Off Contract
"**Service Credit**"	means a sum to be credited by the Supplier to the Buyer for a failure to achieve a Service Level, as calculated and agreed in the Call-Off Contract by the Parties;
"**Service Definition"**	means the Supplier's description of the Services, published by the Supplier on the Framework Contract Digital Marketplace, which sets out the material information required to enable a public sector buyer to understand, evaluate, and compare the Services. The Service Definition serves as a core reference for service selection and supports transparency, compliance, and interoperability under the Framework Contract
"**Service Elements**"	means the Services, the Supplier Environment, the Supplier Content and the Third-Party Elements (including but not limited to Third-Party Environment, the Third-Party Content, and the Third-Party Services);
"**Service Level**"	means a target performance standard set out in the Call-Off Contract, the Service Definition and/or the General SLA Terms (as the case may be) in accordance with which the Supplier shall provide the Service to which it relates;
"**Severity Level**"	means the severity level of the Incident, which has been allocated by the Supplier in accordance with criteria detailed in the Call-Off Contract or the Service Definition (as the case may be);

"**Shared Environment**"	means a services infrastructure that hosts and performs services in respect of multiple end customers of Supplier;
"Specification"	means the technical and functional specifications for the operation of the Services, as in indicated in the Service Definition Documents
"**Submissions**"	means all submissions, feedback and/or suggested improvements to the Service Elements that the Buyer or any End User provides to the Supplier;
"**Supplier Content**"	means the Content that the Supplier or any of the Supplier's Associated Companies owns and makes available in connection with or as part of the Service Elements;
"Supplier Environment"	means the hardware and other equipment, communications and other IT infrastructure of the Supplier or its Associated Companies made available by the Supplier in connection with, as part of or as a Service;
"**Supplier Parties**"	means the Supplier's Associated Companies, sub-contractors, suppliers, consultants, agents and licensors (including for the avoidance of doubt Supplier Staff and Supplier Subcontractors);
"Tax(es)"	means any tax, however denominated, charge, tariff, contribution, duty, levy, assessment, government charge or fee of any kind charged, imposed or levied, directly or through withholding, by any competent authority (including withholding tax, customs charges and duties and VAT);
"**Third-Party Terms**"	means any terms (including open source licensing terms) in accordance with which, or agreement under which, Third-Party Content, Third-Party Service (including any relevant Subscription Software) and/or a Third-Party Environment (i.e. Third-Party Elements) are made available in connection with or as part of or as a Service by the relevant third party or by the Supplier on such third party's behalf as set out in the Call-Off Contract, the Service Definition or as provided by the Supplier or such third party at the time of the Buyer ordering or accessing and/or using that Service or any time thereafter, as such may be updated by the Supplier or the relevant third party from time to time. Third-Party Terms include some or all (as the case may be) those third-party terms appended to these Supplier Terms in Annex 1, if any;
"Third-Party Content"	means the Content (including open source code) owned and/or made available by any third party (or by the Supplier on such third party's behalf) in connection with, as part of or as a Service;
"Third-Party Elements"	means Third-Party Services and products (including but not limited to IaaS, PaaS, SaaS, Cloud Support Services, software and/or hardware), Third-Party Content and/or a Third-Party Environment made available by a third party (or by the Supplier on such third party's behalf) in connection with, as part of or as a Service;
"Third-Party Environment"	means the hardware and other equipment, communications and other IT infrastructure of a third party (including any Supplier Party who is not an Associated Company of the Supplier) made available by a third party (or by the Supplier on such third party's behalf) in connection with, as part of or as a Service, excluding the Supplier Environment and the Buyer Environment;
"**Third-Party Provider**"	Means any third-party supplier, licensor or services provider of the relevant Third-Party Elements.
"**Third-Party Service**"	means a third-party hosted and/or delivered service made available by the Supplier in connection with, as part of or as a Service;
"**Update**"	means an update to a Service or an IT Service Deliverable that is not systems software or applications software; and
"**Upgrade**"	shall mean a set of systems software or applications software which the Supplier designates as an upgrade to the version licensed to the Buyer under the Call-Off Contract and which may contain minor changes, patches, modifications, enhancements and/or error corrections, save in relation to SaaS where "**Upgrade**" shall have the meaning set out therein.

Annex 1 Third-Party Terms

The third-party terms contained in this Annex shall apply, where expressly referred to in the relevant Order Form, to any Services that utilise, incorporate, or otherwise rely upon the relevant Third-Party Elements. To the extent applicable, these third-party terms shall govern the Buyer's use of those components and shall form part of the Call-Off Contract for the related Services