Service Specific Terms - SaaS Services

1. DEFINITIONS

Data Format: a commercially reasonable, readily available, industry standard and comprehensible electronic format or as may be agreed between the parties

Documentation: user or operating manuals relating to the SaaS Services giving accurate, complete and comprehensible information sufficient for a reasonably competent user to access and use all of the functions of the SaaS Services

Emergency Technology Change: a Technology Change to prevent a Priority Level 1 Incident or to restore SaaS Service availability, prevent further damage from a Priority Level 1 Incident or mitigate material imminent risks

SaaS Incident: an unplanned interruption to the SaaS Services, a reduction in the quality of the SaaS Services or the failure of, or disruption to, an Update that has not yet affected the SaaS Services

SaaS Services: any subscription based solution to be provided under this Agreement including (a) any computer hardware, consumables, operating systems, firmware, telecommunications, networking, routing, cabling, power supplies, electrical or other infrastructure equipment that is used as a platform to host the solution and HSBC Information or is otherwise used in connection with the solution, (b) all computer software and programs developed and/or used by Supplier or any Supplier Personnel in providing the solution which are deployed on the equipment referred to in (a) above and/or are accessed and used (directly or indirectly) as part of the solution, (c) all equipment and storage media used for housing, serving, and maintaining HSBC Information and (d) the information or data accessible on or through such solution **Service Output:** any output generated by or as a result of the SaaS Services or is delivered by or on behalf of Supplier under this Agreement

Priority Level 1 Incident or "P1": a SaaS Incident which has been designated by the parties as “P1” or otherwise / in the absence of designated severity levels having been agreed by the parties constitutes a critical incident with a high impact on the SaaS Services and/or HSBC’s business

Technology Change: any modification, alteration, addition, or removal of technology-related components or processes that impact the provision of the SaaS Services, the functioning of technology infrastructure and/or the Documentation, including but not limited to, Updates, upgrades, configuration adjustments, hardware replacements or network modifications

Update: any additional or amended software or other material (including a patch or fix) which corrects bugs or errors in the SaaS Services and any other update, amendment, upgrade or enhancement (including any AI System) to the SaaS Services that is generally made available to Supplier's customers

2. RIGHTS AND USAGE

2.1 Unless otherwise set out in the Call-Off, the Supplier grants to each HSBC Group Member a non-exclusive, worldwide, irrevocable licence to:

(a) implement, configure and Use the SaaS Services in accordance with this Agreement during the Term;

(b) Use the Service Outputs in accordance with this Agreement on a perpetual basis; and

(c) Use the Documentation during the Term.

2.2 If HSBC has underpaid any Charges and/or any HSBC Group Member has used any SaaS Services, Service Outputs and/or Documentation outside the scope of this Agreement:

(a) Supplier shall notify HSBC of the relevant details; and

(b) Supplier may, as its sole and exclusive remedy, invoice HSBC for such usage at the rates set out in the Call-Off.

2.3 If a HSBC Group Member requires a direct agreement with the Supplier, Supplier will enter into an agreement with the HSBC Group Member confirming that the terms of this Agreement apply and including any additional provisions required by any Applicable Laws.

3. RIGHTS AND OBLIGATIONS

3.1 HSBC shall be account administrator for the SaaS Services and may create all applicable accounts.

3.2 Supplier shall:

(a) provide the SaaS Services, Service Outputs and Documentation in a manner accessible from any network connection;

(b) supply nominated HSBC Personnel with login details, passwords and such other information reasonably required for implementation, configuration, remote access and use of the SaaS Services and the Use of the Documentation and Service Outputs;

(c) not send or store any unlawful data or material; and

(d)

(i) ensure that the SaaS Services do not contain any software to which separate third party terms apply except as listed in the Call-Off; or

(ii) anything capable of deleting HSBC Information, restricting access to the SaaS Services or otherwise rendering any element incapable of unfettered Use (other than passwords).

4. HSBC INFORMATION

4.1 Supplier shall:

(a) provide each HSBC Group Member with continuous access to all HSBC Information in the Data Format and ensure that any formatted HSBC Information remains a complete and accurate copy;

(b) ensure that no HSBC Information is deleted or altered, except by or upon written instruction from HSBC or in accordance with this Agreement, or accessed by any third party

(c) monitor requests for replacement passwords, login details and other information and immediately report any suspicious or unusual request(s) to HSBC;

(d) encrypt, or enable HSBC to encrypt, HSBC Information; and

(e) following termination, provide to HSBC a complete copy of all HSBC Information in the Data Format and not destroy any HSBC Information until HSBC has confirmed in writing that it has a complete copy.

5. WARRANTIES

5.1 Supplier warrants, represents and undertakes that the SaaS Services shall operate substantially in accordance with this Agreement.

5.2 Supplier warrants, represents and undertakes that:

(a) it has the necessary licences, permissions and consents in relation to any third party code (including any open source software) forming part of the SaaS Services to enable use of the SaaS Software as set out in this Agreement;

(b) No third party code (including any open source software) has been combined with, included in, linked to or embedded in the Saas Service, which would require any API or other software combined with, included in, linked to or embedded into the SaaS Service by or on behalf of HSBC:

(i) to be disclosed or distributed to any third party in source-code form;

(ii) to be licensed to any third party for the purpose of making derivative works; and/or

(iii) to be subject to any restrictions regarding the consideration HSBC may charge for distributing such software; and

(c) No other third party code (including any open source software) is required in order for HSBC to have full and unrestricted benefit of the SaaS Services.

5.3 In the event of a breach of clause 5.2 Supplier shall promptly and at its own expense:

(a) procure for HSBC the right to continue to use the Service in accordance with the terms of this Agreement including in compliance with the warranty set out in clause 5.2 above; or

(b) modify the Service so that it complies with the warranty set out in clause 5.2 above

provided that where Supplier modifies the Service, HSBC shall have the same rights in respect of such modified Service as it would have had under the terms of the Agreement in relation to the original Service.

5.4 Failure by Supplier to comply with clause 5.3 shall entitle HSBC to terminate the Agreement.

6. SUPPORT

6.1 Supplier shall support and maintain the SaaS Services during the Term and, as a minimum, shall:

(a) proactively and continuously monitor performance of the SaaS Services and promptly notify HSBC of any actual defect, error, performance failure or anomalies, including any impact on the availability of the SaaS Services, degradation of the SaaS Services or cybersecurity incidents;

(b) make suitably qualified representatives available to respond to technical queries;

(c) subject to paragraph 7, provide and implement all Updates;

(d) keep current and available the relevant Documentation; and

(e) maintain such information or data as may be required to facilitate access and use of the SaaS Services.

7. UPDATES

7.1 Supplier shall discuss its development roadmap and expected Updates with HSBC at least every 3 months, use reasonable endeavours to accommodate HSBC's suggested improvements and keep HSBC regularly informed of its implementation progress.

7.2 Supplier may make reasonable Technology Changes provided that:

(a) Supplier has:

(i) given HSBC's designated contract manager not less than 3 months' prior written notice of the Technology Change, such notice to include:

- a clear and concise description, including the current technology setup, the desired changes, and the reasons;
- an impact assessment of the Technology Change, including potentially impacted systems, functionality, security and performance;
- effective date, time and duration of the proposed Technology Change; and
- a plan for testing and verifying the Technology Change, including a success criteria and rollback plan; and

(ii) provided a test version;

(b) such change does not:

(i) reduce performance, functionality, security or compatibility with HSBC systems;

(ii) reduce any Service Level, Service Credit or HSBC right; or

(iii) increase the applicable Charges or require a material investment in HSBC systems.

7.3 Where HSBC considers a proposed Technology Change will breach paragraph 7.2(b), HSBC may object to the Technology Change in writing and require the Supplier to adjust the Technology Change be required to the Technology Change.

7.4 If the Parties have not agreed the Technology Change in accordance with paragraph 7.3 and the Supplier implements the Technology Change in breach of paragraph 7.2(b) this will be considered a material breach capable of termination under clause 20.1(b).

7.5 Supplier shall carry out maintenance and deploy Updates and Technology Changes within agreed maintenance windows, except for:

(a) emergency maintenance carried out with HSBC's prior written consent; and

(b) Emergency Technology Changes provided that, as soon as possible following the Emergency Technology Change, the Supplier shall:

(i) conduct a review to determine the rationale for the Emergency Technology Change; and

(ii) provide a report to HSBC setting out the steps to be taken by the parties in order to mitigate any requirement for a similar Emergency Technology Change in the future.

8. PENETRATION TESTING

8.1 Supplier shall conduct third-party penetration testing and vulnerability scanning of the SaaS Services, including evidence of data isolation in any multi-tenant services, and provide HSBC with a summary report upon request.

8.2 HSBC may conduct (or appoint a third party to conduct) vulnerability and penetration testing of the SaaS Services.

8.3 If any penetration testing identifies a security failure or that Supplier has failed to perform its obligations under this Agreement, HSBC may require Supplier to rectify the relevant failures.