# Fixed Price Services Agreement

## AGREEMENT

As a result of you ("Customer") and the Hornbill Group company identified in the Order Form ("Hornbill") signing or otherwise accepting an Order Form in connection with fixed price Expert Services, these are the terms (referred to in the Order Form) upon which Hornbill shall supply those services to you. For the avoidance of doubt, there is no contract to supply any such service until the Order Form has been explicitly accepted by Hornbill in writing or electronically.

## 1. DEFINITIONS

In these terms, unless the context otherwise requires, the following words and expressions mean:

"Controller", "Processor", "Processing", "Data Subject", "Personal Data" and "Personal Data Breach" take the meanings given in GDPR;

| | |
|---|---|
| "Data Loss Event" | any event that results, or may result, in unauthorised access to Personal Data held by Hornbill under this agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this agreement, including any Personal Data Breach |
| "Data Protection Legislation" | (i) the GDPR and any applicable national implementing Laws as amended from time to time (ii) the DPA to the extent that it relates to Processing of Personal Data and privacy; and (iii) all applicable Law about the Processing of Personal Data and privacy |
| "Data Subject Access Request" | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data |
| "DPA" | Data Protection Act 2018 and any legislation amending, replacing and/or superseding such act |
| "EEA" | European Economic Area |
| "GDPR" | the General Data Protection Regulation (Regulation (EU) 2016/679) |
| "Information Security Policy" | Hornbill's policies setting out how it manages information security as set out from time to time. The Information Security Policy can be found at https://trust.hornbill.com/security/. Changes to the Information Security Policy will only be made to improve the level of information security provided to Hornbill's Customers |
| "Law" | means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which Hornbill is bound to comply |
| "Protective Measures" | appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measures adopted by it |
| "Sub-processor" | any third Party appointed to perform Processing of Personal Data on behalf of Hornbill in relation to this agreement |
| "Expert Services" | the provision for the Customer by Hornbill or its contractors of technical, training and advisory services as defined in the Statement of Work |
| "Intellectual Property" | any and all copyright and all related rights, neighbouring rights including any rights relating to unauthorised extraction or reutilisation, design rights and any other intellectual property rights whether registered or not |
| "Good Industry Practice" | means the standard of skill, care and knowledge which could reasonably be expected from an experienced person who is in the business of supplying services which are the same as or similar to the services provided under this agreement |
| "Hornbill Intellectual Property" | Intellectual Property owned by Hornbill consisting of original work and materials undertaken by Hornbill either previously or in performing its obligations under these terms |
| "Confidential Information" | Any non-public information relating to either party or its supplier, agents, distributors, subscribers or customers together with any information clearly identified in writing as confidential |
| "Order Form" | any electronic or hard copy document signed or otherwise accepted by the parties in writing (including email) incorporating these terms and setting out the commercial terms upon which the Expert Services are to be supplied to Customer |
| "Statement of Work" | Document that lists and defines all the tasks, activities and deliverables to be delivered for a fixed price under this agreement |
| "Sub-processor" | any third party appointed to perform Processing of Personal Data on behalf of Hornbill in relation to this agreement |
| "Price" | A sum net of VAT agreed by both parties and listed on the Order Form to be paid by Customer to |

Hornbill for the delivery of the Expert Services to achieve the work defined in the Statement of Work onto which VAT at the prevailing rate will be added if applicable

## 2. COMMERCIAL BASIS AND CHARGES

Hornbill shall, subject to and in accordance with these terms and any applicable Order Form provide the Expert Services on a fixed price basis and accomplish the tasks, activities and deliverables set out in the Statement of Work.

## 3. CONFIDENTIALITY

Any Confidential Information which comes into the possession of the other party as a result of the operation of this agreement shall be treated as confidential and shall not be disclosed to any person other than employees of such party requiring such information in pursuance of this agreement, neither shall it be used by the receiving party other than in pursuance of this agreement without the prior written consent of the party to whom it relates. Each party will ensure that employees involved with this agreement are aware of and comply with the provisions of this clause. This clause shall not apply to any information which is in or comes into the public domain other than by a breach of this agreement.

## 4. CUSTOMER OBLIGATIONS

4.1 The Customer shall promptly provide Hornbill with any information the Customer is aware of which Hornbill may reasonably require from time to time to enable it to perform its obligations under this agreement.

4.2 The Customer shall ensure that any deliverables that are their responsibility are delivered within a reasonable time from Hornbill requesting them in writing.

## 5. ACCEPTANCE

5.1 On completion of the Expert Services, Customer shall satisfy itself that the activities, tasks and deliverables as listed in the Statement of Work have been completed in a satisfactory manner. In coming to such a determination Customer may only use criteria reasonably derived from the Statement of Work. If the works undertaken under this agreement are in conjunction with the installation and configuration of a standard software product from Hornbill, for the avoidance of doubt, any acceptance criteria cannot contradict the then standard product documentation unless the criteria are derived explicitly from the Statement of Work.

5.2 Customer shall determine its acceptance of the Expert Services within a reasonable timeframe from the completion of the Expert Services and in any case within a time period of 1 week or 20% of the project duration whichever is the greater.

5.3 If the Customer reasonably determines that it doesn't accept the successful completion of the Expert Services, then it shall clearly document any failures in writing to Hornbill within one week of such determination and shall give Hornbill a reasonable time to rectify the documented issues prior to Customer re-assessing its acceptance of the Expert Services. Following three determinations by Customer that it does not accept the Expert Services, the dispute procedure shall be invoked.

5.4 The Expert Services will be deemed accepted by Customer should Customer fail to notify Hornbill of failure of acceptance within the timelines identified in this clause 5.

## 6. PAYMENT

6.1 Hornbill shall raise an invoice in the amount of the Price on receipt of a purchase order or other such written confirmation from the customer that they wish to proceed with the Expert Services as set out in the Statement of Work.

6.2 Payment terms for all invoices are 30 days.

## 7. VARIATION OF SCOPE OF WORKS

7.1 If Customer wishes to vary the works to be carried out, then it shall communicate the details of the change in writing to Hornbill who will assess the effect of the required change in terms of any increased cost. If there is no increase in cost and subject to any considerations of technical feasibility, Hornbill shall accept and include such a change.

7.2 If in Hornbill's sole reasonable determination the requested change does require an increase in cost, then Hornbill shall communicate same to Customer in writing who if they wish to proceed with the change shall authorize the change and the Price will increase accordingly.

7.3 If Customer wishes to remove items from the Statement of Works Hornbill shall agree to this but the full Price shall still be payable.

## 8. CANVASSING OF STAFF

Neither party shall within a period of six months after the most recent provision of any Expert Services approach directly with a view to employing, engaging or sub-contracting on any basis whatsoever any person who has been involved in this agreement under the employ of the other party.

## 9. TERMINATION

9.1 Either party may terminate these terms by written notice to the other if:

9.1.1 the other party commits any breach of any provision of these terms which is capable of remedy and that other party fails to remedy the breach within 14 days after receipt of a written notice giving full particulars of the breach and requiring it to be remedied

9.1.2 the other party commits any breach of any provision of these terms which constitutes a material breach and which

is not capable of remedy

9.1.3 the other party shall have a receiver or administrative receiver appointed or shall pass a resolution for winding-up (otherwise than for the purpose of a bona fide scheme of solvent amalgamation or reconstruction) or a court of competent jurisdiction shall make an order to that effect or if the other party shall become subject to an administration order (or have an administrator appointed) or shall enter into any voluntary arrangement with its creditors or shall cease or threaten to cease to carry on business

9.2 Should this agreement be terminated by Hornbill in accordance with 9.1 above, then all remaining fees under this agreement being the Price minus any amounts paid by Customer to date become due.

9.3 Should this agreement be terminated by the Customer in accordance with clause 9.1 above then Hornbill shall immediately refund any fees paid in advance by the Customer with respect to services not yet provided by Hornbill under this agreement.

## 10. INTELLECTUAL PROPERTY RIGHTS

10.1 The Hornbill Intellectual Property shall belong to Hornbill absolutely.

10.2 Customer is hereby granted a non-exclusive, irrevocable, perpetual and royalty free licence to use Hornbill Intellectual Property for Customer's own internal use only, provided that such Intellectual Property does not already form part of Hornbill's existing standard commercial software or SaaS suite. For the avoidance of doubt, the use by Customer of such existing standard commercial software or SaaS suite is the subject of a separate agreement or agreements between Hornbill and Customer.

## 11. SERVICE STANDARDS

11.1 Hornbill shall provide the Expert Services in accordance with Good Industry Practice. To the maximum extent permitted by applicable law, Hornbill disclaims all other warranties and conditions, express and implied, including but not limited to implied warranties, conditions and other terms of merchantability, satisfactory quality and/or fitness for purpose with respect to the Expert Services.

## 12. LIABILITY LIMITATIONS

12.1 To the maximum extent permitted by applicable law, neither party shall be liable to the other for:

12.1.1 loss (whether direct, indirect or incidental) of business revenues, business profits, business interruption, loss of business information, or other pecuniary loss;

12.1.2 any consequential, special or indirect loss or damages whatsoever;

12.2 Subject to clause 12.4, in each case, whether arising out of the performance of its obligations under these terms or any Order Form or otherwise, and even if the other party has been advised of the possibility of such damages, each party's maximum liability under this agreement whether for damages for negligence, breach of contract any cause of action in contract, tort or strict liability or otherwise shall be limited to the amount paid or payable by Customer under these terms in the 12 months preceding the event giving rise to such possible damages.

12.3 In the event that any court of competent jurisdiction rules any limitation of liability invalid or unenforceable, the total aggregate liability of the defaulting party shall not exceed the total sum which that party may recover with respect to its liability for such loss or damage under its corporate or organizational insurance(s).

12.4 The exclusions and limitations in this Clause 12 do not apply in respect of (i) death or personal injury caused by the negligence of the other party or its employees acting in the course of their employment, (ii) fraud or fraudulent misrepresentation or (iii) any other liability which cannot be excluded under applicable law.

## 13. DATA PROTECTION

13.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and Hornbill is the Processor. The only Processing that Hornbill is authorised to do is listed in Schedule 1 by the Customer and may not be determined by Hornbill.

13.2 Hornbill shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

13.3 Hornbill shall, in relation to any Personal Data processed in connection with its obligations under this agreement:

13.3.1 unless Hornbill is required to do otherwise by Law, process that Personal Data only in accordance with Schedule 1 as updated from time to time by written agreement of the parties. If it is so required Hornbill shall promptly notify the Customer before processing the Personal Data unless prohibited by Law; and

13.3.2 implement and maintain at its cost and expense Protective Measures as set out in Schedule 2, to safeguard the security of the Personal Data in accordance with Data Protection Laws and protect against a Data Loss Event having taken account of the:

13.3.2.1 nature of the data to be protected; and

13.3.2.2 harm that might result from a Data Loss Event; and

13.3.2.3 state of technological development.

Hornbill will frequently evaluate and tighten, increase or improve such Protective Measures to ensure compliance with Data Protection Legislation and the Protective Measures set out in Schedule 2 may as a result be changed from time to time by Hornbill where such changes are required by best practice, changing technological requirements, to protect against security weaknesses or other such situations that in the reasonable opinion of

Hornbill are required to ensure the Protective Measures remain effective and compliant with Data Protection Legislation. The Customer will be notified in writing when a change is made to the Protective Measures; and

13.3.3 ensure that:

13.3.3.1 Hornbill Personnel do not process Personal Data except in accordance with this agreement (and in particular Schedule 1);

13.3.3.2 it takes all reasonable steps to ensure the reliability and integrity of any Hornbill Personnel who have access to the Personal Data and ensure that they:

13.3.3.2.1 have received adequate training on and comply with Hornbill's duties under this agreement; and

13.3.3.2.2 are in relation to Personal Data subject to a legally binding confidentiality undertaking with Hornbill or any Sub-processor; and

13.3.3.2.3 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement; and

13.3.3.2.4 have undergone adequate training in the use, care, protection and handling of Personal Data.

13.3.4 not transfer Personal Data outside of the EEA or such third countries as the European Commission may from time to time designate unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

13.3.4.1 the Customer or Hornbill has provided appropriate safeguards in relation to the transfer (in accordance with GDPR Article 46) as determined by the Customer; and

13.3.4.2 the Data Subject has enforceable rights and effective legal remedies; and

13.3.4.3 Hornbill complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and

13.3.4.4 Hornbill complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

13.3.5 at the written direction of the Customer, securely delete and / or securely return Personal Data (and any copies of it) to the Customer promptly on termination of this agreement unless Hornbill is required by Law to retain the Personal Data.

13.4 Subject to clause 13.6, Hornbill shall notify the Customer immediately if it:

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

13.4.2 receives a request to rectify, restrict, or erase any Personal Data; or

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

13.4.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement; or

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

13.4.6 becomes aware of a Data Loss Event.

13.5 Hornbill's obligation to notify under clause 13.4 shall include the provision of further information to the Customer in phases, as details become available.

13.6 Taking into account the nature of the Processing, Hornbill shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 13.4 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:

13.6.1 the Customer with full details and copies of the complaint, communication or request; and

13.6.2 such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation; and

13.6.3 the Customer, at its request, with any Personal Data it holds in relation to a Data Subject; and

13.6.4 assistance as requested by the Customer following any Data Loss Event; and

13.6.5 assistance with respect to any data protection impact assessment; and

13.6.6 assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

13.7 Hornbill shall maintain complete accurate and up to date records of all categories of Processing activities carried out on behalf of Customer as required by Data Protection Legislation and information to demonstrate its compliance with this agreement.

13.8 Hornbill shall make available to the Customer on request in a timely manner (and in any event within ten working days) copies of the records under clause 13.7 and such other information as the Customer reasonably requires to demonstrate Hornbill's compliance with its obligations under Data Protection Legislation and this Agreement

13.9 Hornbill shall allow for audits of its Processing activity by the Customer or the Customer's designated auditor and the Customer shall re-imburse Hornbill its reasonable costs at its normal hourly consultancy rate.

13.10 Before allowing any Sub-processor to begin Processing any Personal Data related to this agreement, Hornbill must:

13.10.1 notify the Customer in writing of the intended Sub-processor and Processing; and

13.10.2 carry out adequate due diligence to ensure the Sub-processor is capable of implementing and maintaining the Protective Measures set out in Schedule 2 to this Agreement;

13.10.3 obtain the written consent of the Customer; and

13.10.4 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this agreement such that they apply to the Sub-processor and automatically terminates on the termination of this Agreement; and

13.10.5 provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require. Hornbill has provided a list of its Sub-processors at the date of signing this agreement in Schedule 3 and by signing this agreement the customer is giving its written consent to those Sub-processors Processing Personal Data in accordance with Schedule 1 subject always to the Protective Measures set out in Schedule 2

13.11 Hornbill shall remain fully liable for all acts or omissions of any Sub-processor.

13.12 Hornbill shall indemnify and keep indemnified without limitation the Customer, and vice versa, against all losses, claims, damages, liabilities, costs and expenses (including reasonable legal costs) incurred by it in respect of any breach of this Clause.

13.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Hornbill may on not less than 7 working days' written notice to the Customer amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

## 14. GENERAL

14.1 Entire agreement - Neither party has been induced to enter into these terms by a statement or promise which it does not contain. These terms and any applicable Order Form constitute the entire agreement between Hornbill and the Customer with respect to either party's obligations to the other under these terms or any Order Form and supersedes all previous communications, representations and agreements either written or oral (save for fraudulent misrepresentation) with respect thereto. This shall not exclude any liability which a party would otherwise have to the other party in respect of any statement made fraudulently by that party prior to the date of these terms. The application of any general terms and conditions upon which Customer trades or which it seeks to impose by inclusion in any purchase order or which may arise by way of course of trading or otherwise are excluded and shall be of no effect.

14.2 Assignment - The Customer may not assign, transfer or otherwise dispose of any of its rights or obligations under these terms without the prior written consent of Hornbill such consent not to be unreasonably withheld or delayed. Subject to the foregoing, these terms will bind and inure to the benefit of any successors and assigns. Hornbill may not assign, transfer or otherwise dispose of any of its rights or obligations under these terms without prior notification to the Customer. Hornbill may use subcontractors in the performance of the Expert Services but will remain liable to the Customer for all acts and omissions of its subcontractors as if they were its own under this agreement

14.3 Governing law - This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law and the parties submit to the exclusive jurisdiction of the English courts.

14.4 Separable - Each provision of these terms shall be construed separately and notwithstanding that the whole or any part of any such provision may be held by any body of competent jurisdiction to be illegal invalid or unenforceable the other provisions of these terms and the remainder of the provision in question shall continue in full force and effect. The parties hereby agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable provision which achieves to the greatest extent possible the economic legal and commercial objectives of the invalid or unenforceable provision.

14.5 Relationship between the parties - The relationship of Hornbill to the Customer is solely that of independent contractor, and nothing contained herein is intended or will be construed as establishing an employment, joint venture, partnership, commission agency and or other business relationship between the parties

14.6 Variation - Any variation of these terms or any Order Form must be in writing and signed by an authorised representative of each of the parties. No term or provision hereof will be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented.

14.7 Third party rights - The parties confirm their intent not to confer any rights on any third parties by virtue of this agreement and accordingly the Contracts (Rights of Third Parties) Act 1999 shall not apply to this agreement.

14.8 Dispute resolution - Each party shall use its best endeavours to resolve amicably and expeditiously any dispute which may arise between them concerning these terms, any Order Form or any documents incorporated by reference therein using internal escalation procedures or external meditation as may be agreed. But this clause shall not prevent either party from taking such legal proceedings as it shall decide.

14.9 Force majeure - Notwithstanding anything else contained in these terms, neither party shall be liable for any delay in performing its obligations under these terms or any Order Form if such delay is caused by circumstances beyond its reasonable control and any delay caused by any act or omission of the other party (whether or not such act or omission constitutes a breach of these terms) or a third party provided however that any delay by a sub-contractor or supplier of the party so delaying shall not relieve that party from liability for delay except where such delay is beyond the reasonable control of the sub-contractor or supplier concerned.

14.10 Survival - all provisions of this agreement which by their nature should survive termination shall survive any termination including (without limitation) clauses 3, 8, 9.2, 9.3, 10, 12 and 14.

PARTIES

This agreement is between Hornbill Technologies Limited a company incorporated in England and Wales (registered no. 07244938) whose principal place of business is Apollo, Odyssey Business Park, West End Road, Ruislip, HA4 6QD ("Hornbill") and

**CUSTOMER CONTACT DETAILS**

Full Legal Name "Customer"

Address Line 1

Address Line 2

Town

County

Post Code

Country

Contact Name

Contact Email

SIGNED by the parties

| **Signed on behalf of Hornbill** | **Signed on behalf of the Customer** |
|---|---|
| Signature | Signature |
| Print name | Print name |
| Title | Title |
| Date | Date |

SCHEDULE 1

**Processing, Personal Data and Data Subjects**

1. Hornbill shall comply with any further written instructions with respect to processing by the Customer.
2. Any such further instructions shall be incorporated into this Schedule.

| Description | Details |
|---|---|
| Subject matter of the Processing | The subject of the Processing shall be for the purpose of investigating and resolving customer incidents and issues relating to the Service Management and Collaboration solution and when engaged in paid for value-added Expect Services. |
| Duration of the Processing | Processing will take place until the Termination Date as defined in the Terms of Service and Hornbill may process the data after the Termination Date only as required to comply with clause 13.3.5 of this Agreement. |
| Nature and purposes of the Processing | From time-to-time, in order to progress the investigation of a customer issue, it is required that certain diagnostic assets are reviewed by Hornbill Personnel. This includes, but may not limited to log files, and these diagnostic assets can also contain Personal Data. Hornbill does not provide such information to third-parties not otherwise listed as Sub-processors within the Hornbill Group. With the customer's permission to access their instance, Hornbill Personnel may also progress an investigation into an issue by reviewing their configuration.<br><br>In addition to Support, Hornbill Personnel may also have access to Personal Data whilst working directly on a customer's system during an Expert Services engagement. On such occasions, Personal Data is not transferred or copied.<br><br>Any temporary login information provided to aid these Processing activities is securely stored in an encrypted repository within the Hornbill Offices and strict access controls are applied to limit access to only approved Hornbill Personnel. |
| Type of Personal Data | Personal details (including name, address, date of birth, NI number, telephone number)<br><br>Family, lifestyle and social circumstances<br><br>Education and training details<br><br>Employment details<br><br>Financial details<br><br>Goods or services provided<br><br>Racial or ethnic origin<br><br>Political opinions<br><br>Trade union membership<br><br>Physical or mental health or condition<br><br>Sexual Life<br><br>Offences (including alleged offences)<br><br>Criminal proceedings, outcomes and sentences<br><br>Other (please specify below) |

| | |
|---|---|
| | I have reviewed the Types of Personal Data categories above and have checked all those that will be included in the Personal Data Hornbill will process. |
| Categories of Data Subject | Staff including temporary and casual workers, volunteers and agents<br>Customers and clients (including prospective)<br>Patients<br>Students / Pupils<br>Members of the Public<br>Users (of a specific service, website etc.)<br>Suppliers<br>Industry Third Parties<br>Relatives, guardians and associates of the data subject<br>Advisers, consultants and other professional experts<br>Partners and Resellers<br>Other (please specify below)<br><br>I have reviewed the Categories of Data Subject categories above and have checked all those that will be included in the Personal Data Hornbill will process. |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data | The plan for the return and destruction of the data once Processing is complete is as set out in the Hornbill Terms of Service. |

**Protective Measures - Hornbill Data Security Guide**

**Hornbill Security Policy**

Hornbill Technologies Limited (HTL) is the operating company responsible for hosting the SaaS Service and its supporting infrastructure. The Board of Directors and senior management of HTL have defined an Information Security Policy which provides the governance against which HTL is committed to preserving the confidentiality, integrity and availability of all physical and information assets owned, controlled and Processed by the company. HTL is committed to implementing a Secure Operating Model structured and conformant with the internationally recognised standard for an Information Security Management System (ISMS) ISO/IEC 27001:2013.

**Information Security**

The HTL ISMS is intended to be an enabling mechanism for safeguarding commercially sensitive information and Personal Data Processed within electronic systems and manual filing systems, from accidental, or unlawful destruction, loss, alteration, unauthorised disclosure or access. HTL regularly tests, assesses and evaluates the effectiveness of the ISMS and will from time to time update the ISMS to address new and evolving security threats, technologies and changes to industry standard practices, although no such updates will materially reduce the commitments, protection or overall levels of service provided to the Customer as described herein.

**Risk Management**

3.1. **Risk**. HTL evaluates strategic and operational risks on an ongoing, 'as necessary' basis. Risk assessments are carried out whenever there is a change to any of the Assets as defined at section 7 below (e.g. addition or removal of physical assets), to the scope of the Information Security System, changes to code or to the risk environment.

3.2. The impact that might result from each threat-vulnerability is defined in accordance with the risk assessment methodology against the value of the Asset which the threat-vulnerability combination would exploit and this figure is held for each attribute within the Risk assessment matrix.

3.3. **Vulnerability Management**. HTL as a matter of process undertakes to assess on a regular basis all software and hardware for vulnerabilities identified using industry recognised sources such as vendor information, CVE\NIST lists and internal testing regimes.

3.4. All critical vulnerabilities are either resolved, patched or mitigated by process within the specified timeframe and according to the process as defined in the HTL vulnerability management operating procedure in force at such time.

**Management Systems**

4.1. **Data Protection and Privacy**. HTL is committed to compliance with all national and, where appropriate, international laws relating to the protection of Personal Data and individual privacy (including GDPR); this policy applies to all Personal Data Processed by HTL. Personal Data is classified as Restricted and only accessible on a need-to-use and event-by-event basis; by authorised HTL Personnel who need to deal with it.

4.2. **Compliance with Security Policies and Standards**. HTL continuously reviews and audits operations, security arrangements and controls for compliance, evaluating and implementing appropriate actions to ensure conformance with the ISMS.

4.3. **Penetration Testing.** In addition to regular internal testing HTL contracts third party security organisations, at least annually, to perform penetration testing to identify vulnerabilities and remediation steps that will help to increase the security of the HTL service.

**Mobile Security**

5.1. **Technical Security Measures.** The HTL ISMS defines rigorous policies in respect to mobile security and requires mobile devices (laptops, mobile computers, PDAs, mobile phones, USB sticks and other similar memory devices) to have: (i) password protection, (ii) where appropriate/possible and to be encrypted, (iii) the most recent operating system and application security-related patches, fixes and updates installed.

5.2. **Operational Measures.** HTL requires that; (i) notebook computers are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft this is reported immediately. (ii) users are appropriately trained, understand and can carry out their agreed security obligations.

**HR Security**

6.1. **Personnel Security.** HTL undertakes vetting of Hornbill Personnel with access to Personal Data in line with its current published operating procedures and subject to applicable law(s).

6.2. **Confidentiality.** Employees, with access to Personal Data, are provided with and sign a contract of employment which includes a confidentiality agreement covering the various responsibilities and actions required of signatories in order to avoid unauthorized information disclosure, the permitted use of the information, the signatories' rights in respect of that information and the required actions on termination of the agreement.

**Asset Management**

7.1. **Asset Inventory.** HTL maintains a single inventory of information assets, each of which has defined ownership and is classified as; (i) hardware (all computing and information processing equipment, including printers, fax machines, photocopiers, etc.), (ii) software, information/database (e.g. software, software media etc.), intangible, service (which includes designated secure areas), (iii) people (those individuals whose skills, knowledge and experience are considered essential), and (iv) other assets. This inventory is the asset inventory that is used in the risk assessment process.

7.2. **Asset Ownership.** For each asset, HTL defines the business unit or business role that 'owns' the asset and is therefore responsible for ensuring that the asset is correctly classified and for the day to day maintenance of the identified controls.

**Information Classification & Handling**

8.1. **Information Classification**. HTL classifies information to three (3) levels: restricted, confidential, and public. Information that is classified as restricted must, in addition, identify the individuals or roles to whom the information is restricted. Personal Data subject to Data Protection Legislation is classified as restricted and is subject the policies as documented in the HTL operating procedure for Information Classification and Handling.

**Access Control**

9.1. **Access Management.** Access to the SaaS Service from HTL is by Hornbill Personnel and Sub-processors is secured, managed and protected through stringent authentication, segregation and authorisation processes and mechanisms, overseen by the HTL ISMS manager. A formal registration and deregistration process is adhered to and privileges are allocated on a need-to-use and event-by-event basis. A log is maintained of all privileges authorised and allocated and this is audited regularly to ensure privileges; (i) have been revoked as specified in the original request, (ii) continue to be valid and appropriate for the intended purpose, (iii) have not been obtained without the appropriate authorisation. User access rights are reviewed upon change to maintain effective control over access to data information services.

9.2. **Technical and Network Access Controls.** HTL employs a wide range of measures and controls including, but not limited to; (i) Secure log-on, (ii) Network access controls, including VPN's and Firewalls with controlled ports. (iii) Network segregation with defined inter-network connection protocols and routing. (iv) Real time monitoring and logging against HTL instances and infrastructure to detect logins, unusual access and or unexpected data transfers. (v) Logs are reviewed (automatically) for warnings and corrective actions taken to address any concerns (For example, any port scanner or other bot probing would be blocked from all access).

9.3. **Service Access Controls.** The SaaS Service provides extensive and granular user and role-based access controls. The Customer is solely responsible for the management, configuration and confidentiality of such access controls within its HTL instance and must assign to each user secure credentials and user role controlling the individuals level of access to the SaaS Service.

**Cryptography Controls and Usage**

10.1. **Data Encryption.** All data is encrypted in transit, and where possible specific fields are encrypted at rest using industry recognised cryptographic measures, TLS Encryption. All backups are fully encrypted. All data in motion is encrypted either via HTTPS\SSL.

10.2. Full at rest encryption (AES-256), of the Customers HTL instance, is available to Customer subscribed to the SaaS Service running on the HTL Platform Enterprise Edition.

**Physical and Environment Security**

11.1. **Data Centre Facilities**. HTL delivers the SaaS Service from data centres within the Customers chosen Hosting Zone (data protection jurisdiction) that have attained SSAE16 and ISO27001 certification.

11.2. Physical access restrictions in place will include a combination of any of the following: External and internal CCTV systems, proximity access controls, access card biometric authentication, mantrap, intruder alarms, door tampering alarms, appropriate perimeter deterrents (e.g. fencing, guarded gates), on site guards and secure managed loading dock; and (ii) fire suppression and detections systems in all areas.

11.3. **Secure Management and Disposal of Equipment**. Assets. The HTL Chief Technical Officer is responsible for the secure disposal of storage media and the disposal of all information processing equipment. Destruction of storage media and information processing equipment is undertaken to industry standards with the physical destruction of decommissioned or damaged hard disks storing Personal Data undertaken line with WEEE regulations through HTL's approved contractor.

**Operations**

12.1. **Capacity Management.** Network capacity, utilisation, disk utilisation and load are proactively monitored, with automated alerting, to ensure that the SaaS Service has sufficient capacity of current and anticipated needs.

12.2. **Monitoring.** Each HTL instance is monitored from multiple locations globally with checks on over one hundred individual metrics undertaken every five minutes including but not limited to; (i) Performance (Pings, DNS Propagation, Response times from API, CPU Load, RAM Load, Disk IO, network Load etc.), (ii) Hardware (Availability, Temperature, SMART, SNMP etc.), (iii) Capacity (Disk space, CPU, Ram, etc.), (iv) Availability (Ping, DNS Propagation, API Tests, Host controller checks etc.), (v) Security (Automated Log file reviews, Traffic review, Pattern analysis, etc.), (vi) IDS (Intrusion Detection, Suspicious or Malicious Traffic Analysis including, packet \ bandwidth \ source \ traffic monitoring), (vii) Data Leakage ( Packet\bandwidth\Source & Destination \ traffic monitoring and Analysis), (viii) Backups (Sync checks, replication checks, off instance checks etc.) and, (xi) Sanity (Checks for Mail Queues, Expected load etc.).

**Supplier Relationships and Procurement**

13.1. HTL carries out risk assessments to identify and implement specific controls before granting access to third parties or customers in line with the published operating procedures in force at such time. Identification of risk related to external party access takes account of the following: (i) level of physical access, (ii) logical access, (iii) legal and regulatory requirements and other contractual obligations relevant to the external parties. HTL defines and agrees with the external party those controls that the external party is required to implement and documents them in a signed contract or agreement.

**Incident Reporting\Handling and Management**

14.1. **Incident Reporting and Handling.** HTL will monitor for, analyse and respond to information security incidents immediately they are seen or experienced and report all such incidents to the Information Security Manager who will be responsible for undertaking an assessment and categorising the reported incident in a timely manner and in accordance with HTLs documented operating procedures.

14.2. **Notification of Breach.** HTL shall report to the Customer any; access to, alteration, disclosure of, accidental or unlawful destruction, or loss to Personal Data (a "Breach") in accordance with Clause 9.4 of this Agreement.

14.3. **Report.** An initial report shall be made to the Customers authorised contact(s) as maintained by the Customer in respect to the specified HTL instance. As HTL investigates or otherwise becomes aware of further information, and unless restricted by any applicable law, it shall provide all further information pertaining to the nature and impact of the Breach such that the Customer may be able to subsequently notify relevant parties concerned be that; Data Subjects, government agencies and data protection authorities in line with Data Protection Legislation.

**Change Reporting\Handling\Planning and Management**

15.1. **Change Management.** The Chief Technical Officer or Cloud Service Manager in consultation is responsible for authorising changes. Changes are not approved for implementation until fully risk assessed and where required defined fall-back procedures or a roll back strategy must be prepared. Where the change is significant, a testing plan, complete with clear acceptance criteria (including business, technical and load criteria) must be documented prior to commencing the change testing, which may include a dry run of the change.

15.2. **Promotion to Production Environment.** All testing is conducted in a test environment which is configured for that specific test requirement. This is separated from operational facilities by logical means. Once proved to be effective the HTL Cloud Service Manager authorises the implementation of the change to the operational environment, ensuring that business processes are not disturbed and that business continuity plans are updated if appropriate.

**Business Continuity and Disaster Recovery**

16.1. **Business Continuity**. HTL are committed to providing customers with access to the SaaS Service and data even in the event of an emergency or disaster. HTL's emergency plan is designed such that in the worst possible case Customers will be without access to instances for the minimum time possible whilst a full restore is carried out to a secondary data centre.

16.2. **Backups.** All databases relating to the SaaS Service are replicated in real time to a secondary data centre. All files are replicated every 5 minutes. Replicas are subsequently backed up (individual secure archive encrypted with 1-time key) daily and stored in a tertiary location within the Customers contracted hosting zone. The backups are taken without any interruption of services.

SCHEDULE 3

**Sub-processors**

Hornbill use the Sub-Processors as listed from time to time on the Hornbill Wiki which can be found here https://wiki.hornbill.com/index.php/FAQ:Subprocessors