Hornbill Subscription Agreement

AGREEMENT

As a result of you ("Customer") and the Hornbill Group company identified below ("Hornbill") signing or otherwise accepting this agreement in connection with the provision of the Hornbill SaaS Service, these are the terms upon which Hornbill shall supply those services to you.

DEFINITIONS

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

"Billing Commencement Date"	the date the Customer requests the SaaS Service is made available as stated on the Order Form or the date the SaaS Service is made available to the Customer by Hornbill whichever is the later
"Billing Period"	the length of time each invoice covers as stated on the Order Form
"Community Forum"	a public forum in which questions can be asked about the configuration and use of the system. Posts on the Community Forum will be monitored by Hornbill employees who will respond when appropriate
"Confidential Information"	any non-public information relating to either Party or its suppliers, agents, distributors, subscribers, employees or customers together with any information clearly identified in writing as confidential. All Customer Data shall be treated as Confidential Information except as otherwise set out in this agreement

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

"Customer Data"	information, data, editorial content, Intellectual Property in any form relating to the Customer, including without limitation, its employees, customers, business and activities, including Protected Data or such data otherwise governed by applicable Data Protection Legislation, posted or submitted to the SaaS Service by a User or by Hornbill Personnel on behalf of Customer
"Data Loss Event"	any event that results in unauthorised access to Personal Data held by Hornbill under this agreement, and/or loss and/or destruction of Protected 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 or replaced from time to time (ii) the UK GDPR (iii) the DPA to the extent that it relates to Processing of Personal Data and privacy; and (iv) all applicable Law about the Processing of Personal Data and privacy in any relevant jurisdiction
"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) and General Data Protection Regulation (Regulation (EU) 2016/679)
"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
"Group"	means the Customer together with its holding company or companies and any subsidiary or subsidiary undertaking of the Customer or any such holding company, from time to time
"Hornbill Personnel"	means all directors, officers, employees, agents, consultants and contractors of Hornbill and/or of any sub-contractor engaged in the performance of its obligations 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
"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/. Changes to the Information Security Policy will only be made to improve the level of information security provided to Hornbill's Customers
"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
"Knowledge"	means the product documentation, learning materials, and other knowledge-based resources made available by Hornbill to the Customer from time to time, including but not limited to the Hornbill Docs site (https://docs.hornbill.com/) and the Hornbill Academy.

"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
"Order Form"	any electronic or hard copy document signed or otherwise accepted by the parties incorporating these terms and setting out the commercial terms upon which the SaaS Service is supplied to Customer
"Party"	a Party to this agreement
"Protected Data"	means Personal Data received from or on behalf of the Customer or otherwise obtained in connection with the performance of Hornbill's obligations under this agreement
"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
"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations 2004
"SaaS Service"	the provision of the Hornbill platform and one or more configurable business applications, enabling the Customer to design, automate, and manage workflows and data-driven processes.
"Service Credits"	credits due to Customer as published from time to time here https://docs.hornbill.com/hornbill-customer-services/success-plans/essential-success
"Service Levels"	the service levels for the SaaS Service published by Hornbill from time to time here https://docs.hornbill.com/hornbill-customer-services/success-plans/essential-success
"Service Parameters"	the system resources and any other parameters or limits of the SaaS Service as contained in any Order Form and as detailed from time to time here https://docs.hornbill.com/hornbill-customer-services/success-plans/service-parameters
"Sub-processor"	any third party appointed to perform Processing of Personal Data on behalf of Hornbill in relation to this agreement
"Subscription Fee"	the fees and charges as defined in an Order Form or as amended by clause 9 of this agreement to be paid by the Customer to Hornbill under these terms for the SaaS Service for any Billing Period
"Subscription Period"	is the length of time the Customer is committing to continue paying for the SaaS Service as set out in the Order Form
"Essential Support"	access to the Community Forum, Knowledge and 24 x 7 x 365 support for critical issues relating to the availability of the SaaS service. Details of the Essential Support service can be found here https://docs.hornbill.com/hornbill-customer-services/success-plans/essential-success
"Termination Date"	either the date the Customer tells Hornbill it wants the SaaS Service switched off or the date Hornbill advises the Customer it is switching off the SaaS Service in accordance with this agreement
"Trade Marks"	Hornbill's own corporate, trade and product branding, trade marks, service marks or other similar Intellectual Property rights owned by Hornbill from time to time
"UK GDPR"	means as defined in section 3(10) (as supplemented by section 205(4)) of the DPA
"User"	any person who connects to the SaaS Service whether or not they have a paid subscription

1. COMMERCIAL BASIS

1.1. Subject to and in accordance with these terms and any applicable Order Form after the Billing Commencement Date Hornbill shall:

1.1.1. provide the SaaS Service and the Essential Support in accordance with:

1.1.1.1. Good Industry Practice; and
1.1.1.2. The Service Parameters; and
1.1.1.3. the Service Levels; and
1.1.1.4. all reasonable instructions of the Customer; and
1.1.1.5. all applicable law and regulations; and

1.1.2. from time to time update the SaaS Service to a more recent or the most recent version of the Hornbill software; and

1.1.3. no more than once per quarter on request provide Customer with a copy of the most recent Customer Data in an industry standard machine readable format as determined by Hornbill.

1.2. The Subscription Fee for the SaaS Service shall be paid by the Customer in accordance with the Service Parameters.

1.3. Customer shall be due Service Credits following any failures of the SaaS Service to meet the Service Levels.

1.4. The first Subscription Period commences on the Billing Commencement Date.

1.5. Hornbill shall raise an invoice in the amount of the Subscription Fee for the first Billing Period on receipt of the first Order Form.

1.6. Hornbill shall raise subsequent invoices in the amount of the Subscription Fee in respect of future Billing Periods no more than 45 days before the current Billing Period ends until the first Subscription Period ends.

1.7. If Customer wishes to continue to use the SaaS Service after the end of any Subscription Period the Customer does not need to take any action. At the end of the Subscription Period a new Subscription Period with a duration of one year and with a Billing Frequency of one year will be entered on the otherwise same terms, subject to any price changes, as the previous Subscription Period.

1.8. At any time before the end of a Subscription Period if the Customer would like to change the Subscription Period or Billing Period for the next Subscription Period the Customer must sign a new Order Form stating the revised Subscription Period and Billing Period. For the avoidance of doubt if the Subscription Period or Billing Period are changed the Subscription Fee may also change.

1.9. In the event of a change in the Subscription Period or Billing Period under clause 1.8 Hornbill shall raise the invoice for the Subscription Fee as soon as practicable having cancelled any invoices that were raised under Clause 1.7.

1.10. Fees for Services are exclusive of Value Added Tax (VAT) or other Government imposed excises or taxes (if any) which shall be paid by the Customer at the rate and in the manner for the time being prescribed by Law.

1.11. Invoices are due for payment within 30 days.

2. CUSTOMER KEY RESPONSIBILITIES AND SERVICE USE

2.1. Customer shall:

2.1.1. when accessing the SaaS Service follow any reasonable technical and operational guidelines of which Customer is notified by Hornbill; and
2.1.2. provide reasonable support to Hornbill in managing and monitoring of the quality of the SaaS Service and in planning and implementing any agreed enhancements to the SaaS Service; and
2.1.3. shall protect and keep confidential the login credentials that each User uses to access the SaaS Service, to a standard not lower than it generally uses across its business to protect access to its own computer systems; and
2.1.4. shall ensure that any User's usage of the SaaS Service does not result in a breach of the terms of this agreement; and
2.1.5. provide any necessary payment reference number or purchase order number as required by its own internal processes to ensure Hornbill's invoices are paid within the agreed terms. Failure to provide this data will not be grounds for a bona fide dispute in clause 6.5.

2.2. The Customer acknowledges and agrees that it is solely responsible for complying with any laws or paying any taxes duties and tariffs applicable in any way to its use of the SaaS Service (other than taxes on the net income of Hornbill).

2.3. The Customer unconditionally represents warrants and undertakes that all Customer Data:

2.3.1. is owned by the Customer or that the Customer has permission from the rightful owner to use Customer Data in the SaaS Service and that the Customer Data is in no way whatsoever a violation or infringement of any third party Intellectual Property, right of privacy or publicity or any other rights of any person; and
2.3.2. is not obscene, libellous or defamatory or in any other way unlawful; and
2.3.3. is to the best of its knowledge free of viruses and other malware and that it employs virus and malware protection procedures of no lower standard than it uses to protect the integrity of its own computer systems.

2.4. The Customer represents and warrants that:

2.4.1. it will use the SaaS Service for lawful purposes only and in accordance with all applicable laws, regulations and licences; and
2.4.2. it will not attempt to decompile, reverse engineer or hack the SaaS Service or to defeat or overcome any encryption and/or other technical protection methods implemented by Hornbill; and
2.4.3. it will not use any automatic or manual device or process nor take any steps, including penetration testing, to interfere with or in any manner compromise any security measures or the proper working of the SaaS Service; and
2.4.4. it will not use any other individual's or entity's login or identity or any other unauthorised method to access or use the SaaS Service; and
2.4.5. It will not attempt to exceed any limits imposed by the Service Parameters nor take any steps to interfere with or compromise any methods implemented by Hornbill to monitor and enforce the Service Parameters; and
2.4.6. it will not collect any information or communication about Hornbill or other Hornbill customers by monitoring, interdicting or intercepting any process of the SaaS Service.

2.5. The Customer hereby agrees that any user interface form elements, menu's, labels, tooltips or help content that is translated by the Customer may be accessed by Hornbill and combined with other Customer's translation data to produce default product translations which may be made available to all customers. For the avoidance of doubt this does not apply to any other Customer Data entered into the system which remains fully private to the Customer's instance.

3. RIGHTS IN SERVICES AND DATA AND INDEMNITY

3.1. The Customer acknowledges and agrees that Hornbill product comprising or within the SaaS Service, consists of original work and materials undertaken by Hornbill either previously or in performing its obligations under these terms. The Customer acknowledges and agrees that the copyright and all other intellectual property rights in such Hornbill Intellectual Property whenever created shall remain the exclusive property of Hornbill and the Customer shall have no rights in respect thereof save as may be granted to it by Hornbill pursuant to these terms or in accordance with any licence or agreement which Hornbill may enter into with the Customer from time to time. The Customer agrees to use the Hornbill Intellectual

Property only as provided in these terms and to not use it to develop software for third parties or for any other purpose without the prior written authorisation of Hornbill. The Customer will take all reasonable steps to protect the intellectual property rights of Hornbill in the Hornbill Intellectual Property.

3.2. Hornbill acknowledges and agrees that copyright in Customer Data may belong to the Customer or a third party and for the avoidance of doubt asserts no claim pursuant to these terms inconsistent with any such rights.

3.3. The Customer shall not:

3.3.1. remove or interfere with any Trade Marks, copyright or Trade Mark notices affixed or installed by Hornbill on the SaaS Service or other Hornbill Intellectual Property except where the service allows such supported configurations; and

3.3.2. use the SaaS Service to provide or be part of any commercial external service to sub-tenants. For the avoidance of doubt, the Customer may use the SaaS Service to provide services to any companies within its Group.

3.4. The Customer acknowledges and agrees that the SaaS Service may use User activity monitoring and metering software to avoid any violation of licence or service usage terms and to protect Hornbill against unauthorised, unlicensed or illegal use of the SaaS Service.

3.5. Hornbill shall indemnify the Customer against any claims or loss suffered by the Customer as a result of a claim that the SaaS Service (except for any Customer Data) infringes the intellectual property rights of any third party and the Customer shall indemnify Hornbill against any claims or loss suffered by Hornbill as a result of a claim that any Customer Data supplied by the Customer and incorporated into or used with the SaaS Service infringes the intellectual property rights of any third party provided that the Party claiming indemnity shall:-

3.5.1. immediately notify the other on becoming aware of any such claim; and

3.5.2. not take any other action in respect of such claim or make any admission or settlement of any such claim without the other's prior consent in writing; and

3.5.3. subject to being indemnified by the other against the reasonable costs and expenses of the Party claiming indemnity take all such actions in relation to such claim as the other shall properly require.

3.6. Without prejudice to Clause 3.5, Hornbill shall be entitled to make such modifications to the SaaS Service as shall avoid any infringement of any third party's intellectual property rights for which it is liable to indemnify the Customer under this agreement provided such modifications do not materially adversely affect the functionality of the SaaS Service.

4. LIABILITY AND LIMITATIONS

4.1. To the maximum extent permitted by applicable law, neither Party shall be liable to the other for:

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

4.1.2. any consequential, special or indirect loss or damages whatsoever.

4.2. 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 actually paid by Customer in the case of default by Hornbill, or shall be limited to the amount payable by Customer in the case of default by Customer under these terms in the 12 months preceding the event giving rise to such possible damages.

4.3. 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).

4.4. The exclusions and limitations in this Clause 4 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. (iii) breach of Data Protection legislation (iv) breach of Intellectual Property Rights or (v) breach of the provisions of clause 10 (Prevention of Fraud and Corruption) or (v) any other liability which cannot be excluded under applicable law.

4.5. Hornbill does not represent or warrant that the SaaS Service will always be available, accessible, uninterrupted, timely, secure, accurate, complete, error-free, or will operate without data loss, nor does Hornbill warrant or guarantee any connection to or transmission from the internet.

5. CONFIDENTIALITY

5.1. Subject to the provisions of clauses 5.7 and 5.8 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 shall 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.

5.2. Customer may from time to time provide suggestions, comments or other feedback ("Suggestions") to Hornbill concerning the SaaS Service. Both parties agree that all Suggestions are and shall be given entirely voluntarily. Except as otherwise provided herein, Hornbill shall be free to use, disclose, reproduce, license or otherwise distribute, and exploit the Suggestions provided to it as it sees fit, entirely without obligation or restriction of any kind on account of intellectual property rights or otherwise. All Suggestions will be anonymous if shared with third parties unless the Customer gives its prior written approval to be associated with the Suggestions.

5.3. Hornbill may access and process Customer Data posted by or on behalf of the Customer or in connection with the SaaS Service as reasonably necessary to operate or maintain the SaaS Service and to comply with obligations of confidentiality Hornbill has to the Customer or other customers.

5.4. Hornbill may monitor the Customer's usage to evaluate or improve the performance and implementation of and to promote and market SaaS Service and to measure, amongst other things, interest in and use of SaaS Service and to develop and design new products and services.

5.5. Hornbill shall take such technical and organisational measures against the unauthorised or unlawful processing of Customer Data and against accidental loss or destruction of, or damage to, Customer Data as set out from time to time in its Information Security Policy.

5.6. Hornbill shall indemnify and keep indemnified the Customer, and vice versa, against all losses, claims, damages, liabilities, costs and expense (including reasonable legal costs) incurred by it in respect of any breach of this Clause 5 or any act or omission of any sub-contractor.

5.7. Notwithstanding clause 5.1, a Party may disclose Confidential Information which it receives from the other Party:

5.7.1. where disclosure is required by applicable law or by a court of competent jurisdiction;
5.7.2. to its auditors or for the purposes of regulatory requirements;
5.7.3. on a confidential basis, to its professional advisers;
5.7.4. to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;
5.7.5. where the receiving Party is Hornbill, to the Hornbill Personnel on a need to know basis to enable performance of Hornbill's obligations under the agreement provided that Hornbill shall procure that any staff to whom it discloses Confidential Information pursuant to this clause 5.7.5 shall observe Hornbill's confidentiality obligations under the agreement; and
5.7.6. where the receiving Party is the Customer:

5.7.6.1. on a confidential basis to the employees, agents, consultants and contractors of the Customer; or
5.7.6.2. to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its functions; or
5.7.6.3. in accordance with clauses 5.8.1 to 5.8.4,

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Customer under this clause 5.

5.8. Notwithstanding clause 5.1 where the Customer is subject to the Freedom of Information Act 2000 (FOIA) this clause 5.8 shall apply.

5.8.1. The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this agreement is not Confidential Information and Hornbill hereby gives its consent for the Customer to publish this agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the agreement agreed from time to time. The Customer may consult with Hornbill to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the agreement is exempt from disclosure in accordance with the provisions of the FOIA.

5.8.2. Hornbill acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:

5.8.2.1. provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
5.8.2.2. transfer to the Customer all Requests for Information relating to this agreement that it receives as soon as practicable and in any event within 2 working days of receipt;
5.8.2.3. provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its possession or control in the form that Customer requires within 5 working days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and
5.8.2.4. not respond directly to a Request for Information unless authorised in writing to do so by the Customer.

5.8.3. Hornbill acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning Hornbill or the SaaS Service and the Support Service and any other ancillary services (including commercially sensitive information) without consulting or obtaining consent from Hornbill. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give Hornbill advance notice, or failing that, to draw the disclosure to Hornbill's attention after any such disclosure.

5.8.4. Notwithstanding any other provision in the agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to Hornbill or the SaaS Service or Support Service or any other ancillary services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004

6. TERM TERMINATION AND SUSPENSION

6.1. Unless otherwise agreed in writing the SaaS Service shall continue only during such Subscription Periods in respect of which the applicable Subscription Fee shall have been paid in full to Hornbill unless and until terminated under clause 6.2 or 6.3.

6.2. Customer may terminate this agreement on or after the expiry of any Subscription Period by providing at least 7 days notice in advance of the expiry of the Subscription Period to Hornbill of its preferred Termination Date such date must be on or after the expiry of the current Subscription Period. On receipt of such notice Hornbill shall acknowledge the notice with 48 hours. If the Termination Date is after the end of a Subscription Period Hornbill shall raise an invoice for the pro rata amount of the Subscription Fee to the Termination Date. Any further extensions to the Termination Date that the Customer may request will be agreed to by Hornbill subject to a minimum term of 3 months.

6.3. Either Party may terminate these terms by written notice to the other Party if:

6.3.1. the other Party commits any breach of any provision of these terms or an Order Form which is capable of remedy (including for the avoidance of doubt any breach referred to in clause 6.3.2) and the Party committing the breach 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; or

6.3.2. the other Party commits any breach of any provision of these terms which constitutes a material breach (material breach for this purpose meaning a breach that has caused or, with the passage of time, will cause substantial harm to the interests of the innocent Party or if it involves knowing and unauthorised infringement of the innocent Party's Intellectual Property, or if it involves knowing or grossly negligent unauthorised disclosure or use of the innocent Party's Confidential Information, or if it involves a continuing failure after warning to pay any undisputed fees when due, or if the aggregate effect of non-material breaches by the Party committing the breach satisfies these standards for materiality); or

6.3.3. 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.

6.4. Upon any termination of these terms:

6.4.1. Hornbill will before deletion of the Customer Data as provided in 6.4.2 provide the Customer with a copy of the most recent Customer Data in an industry standard machine readable format as determined by Hornbill; and

6.4.2. Hornbill will delete the Customer Data between 30 and 60 days after the Termination Date; and

6.4.3. subject as otherwise provided in these terms and to any rights or obligations which have accrued prior to termination, neither Party shall have any further obligation to the other under these terms except that all provisions of this agreement which by their nature should survive termination shall survive any termination including (without limitation) : 2.5, 4, 5, 7.4, 7.5, 7.6, 7.8, 8.2 and 8.6.

6.5. Customer acknowledges and agrees that if any invoice (not subject to a bona fide dispute) is not paid on the due payment date then Hornbill reserves the right to suspend Customer access to the SaaS Service. Prior to suspension Hornbill will notify Customer of its intent to suspend access and Hornbill will not suspend the service until at least 14 calendar days (30 calendar days in the case of Subscription Fee invoices subsequent to the first Subscription Fee invoice) have elapsed after the first notice of suspension. Hornbill will remove the suspension once Customer has paid all due invoices not subject to a bona fide dispute.

7. GENERAL

7.1. 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 constitutes the entire agreement between Hornbill and the Customer with respect to the supply of SaaS Service 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 the Customer trades or which it seeks to impose by inclusion in any purchase order or by way of course of trading or otherwise are excluded and shall be of no effect.

7.2. 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.

7.3. Hornbill may use subcontractors in the performance of the SaaS Service but will remain liable to the Customer for all acts and omissions of its subcontractors as if they were its own under this agreement.

7.4. Governing law – This agreement shall be governed by and construed in accordance with English law and the parties submit to the exclusive jurisdiction of the English courts.

7.5. 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.

7.6. 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.

7.7. 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.

7.8. 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.

7.9. 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 mediation as may be agreed. But this clause shall not prevent either Party from taking such legal proceedings as it shall decide.

7.10. 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.

7.11. Warranties – Hornbill warrants, represents and undertakes on an on-going basis that:

7.11.1. it has, and shall continue to have, full ability, capacity and authority to enter into and perform its obligations under this agreement;
7.11.2. it has all authorisations required by Applicable Laws and Regulations to provide the SaaS Services; and
7.11.3. it is not a party to any contracts or arrangements with third parties that would prevent or hinder the performance of its obligations under this agreement.

8. DATA PROTECTION

8.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and Hornbill is the Processor of any Protected Data.

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

8.3. Hornbill shall, in relation to any Protected Data processed in connection with its obligations under this agreement:

8.3.1. process that Protected Data only in accordance with Data Protection Legislation, this Clause 8 and the documented instructions in Schedule 1 as updated from time to time by written agreement of the parties, unless Hornbill is required to do otherwise by applicable law, in which case Hornbill shall, unless legally prohibited from doing so, notify the Customer before processing the Personal Data; and
8.3.2. implement and maintain Protective Measures as set out in Schedule 2, to safeguard the security of the Personal Data in accordance with Data Protection Legislation and protect against a Data Loss Event having considered:

8.3.2.1. the nature of the data to be protected; and
8.3.2.2. the harm that might result from a Data Loss Event; and
8.3.2.3. the state of technological development.

8.4. The Parties acknowledge that the adequacy of the Protective Measures mentioned in this clause 8.3 and Schedule 2 may change over time, and that an effective set of Protective Measures demands frequent evaluation and improvement of Protective Measures. Therefore 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 Hornbill shall

8.4.1. ensure that Hornbill Personnel who are authorised to process Protected Data are subject to appropriate obligations of confidentiality; and,

8.4.2. ensure that Protected Data that is transferred outside of the UK or EEA satisfies the requirements contained in applicable Data Protection Legislation; and,

8.4.3. 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.

8.5. Subject to clause 8.6, Hornbill shall notify the Customer if it:

8.5.1. receives a Data Subject Access Request (or purported Data Subject Access Request); or
8.5.2. receives a request to rectify, block or erase any Personal Data; or
8.5.3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation; or
8.5.4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Protected Data processed under this Agreement; or
8.5.5. receives a request from any third party for disclosure of Protected Data where compliance with such request is required or purported to be required by Law; or
8.5.6. becomes aware of a Data Loss Event.

8.6. Hornbill's obligation to notify under clause 8.5 shall include the provision of further information to the Customer in phases, as details become available.

8.7. Considering the nature of the Processing, Hornbill shall provide the Customer with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 8.5 (and insofar as possible within the timescales reasonably required by Data Protection Legislation) including by providing:

8.7.1. the Customer with full details and copies of the complaint, communication or request; and
8.7.2. 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
8.7.3. the Customer, at its reasonable request, with any Personal Data it holds in relation to a Data Subject; and

8.7.4. such assistance as reasonably requested by the Customer following any Data Loss Event; and
8.7.5. such assistance with respect to data protection impact assessments in relation to this agreement; and
8.7.6. such 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.

8.8. 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 and shall provide reasonable assistance to the Customer with any data protection impact assessments.

8.9. 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 8.8 and such other information as the Customer reasonably requires to demonstrate Hornbill's compliance with its obligations under Data Protection Legislation and this agreement

8.10. Hornbill shall allow for and contribute to audits of its Processing activity by the Customer or the Customer's designated auditor no more than once per calendar year (except where there has been a Data Loss Event in which case this is permitted) and each party shall be responsible for its own costs provided that:

8.10.1. reasonable advance notice shall be given in respect of any such audit; and
8.10.2. any such audit shall only be conducted during Hornbill's normal business hours; and
8.10.3. any such audit shall be conducted to cause minimal disruption to the Hornbill's business operations; and
8.10.4. no access shall be given to Hornbill's confidential information or any information relating to Hornbill's other clients and/or financial data; and
8.10.5. any third party auditor shall enter into confidentiality obligations directly with Hornbill which are reasonably acceptable to Hornbill.

8.11. The Customer agrees that Hornbill engages Sub-processors in connection with the provision of the Services and that the list of the Sub-processors currently engaged by Hornbill is listed here https://docs.hornbill.com/hornbill-cloud/subprocessors. Therefore, by entering to this agreement, Customer authorises Hornbill to engage the Sub-processors mentioned in this list to Process the Protected Data in accordance with Data Protection Legislation and Schedule 1 subject always to the Protective Measures set out in Schedule 2.

8.12. The Customer further provides its general authorisation for Hornbill to engage other Sub-processors, add or replace the Sub-processors in the list. At least fourteen (14) calendar days before authorising any new Sub-Processor to access Protected Data Hornbill will notify Customer of the proposed change to the list. Customer can object to such changes by contacting data.privacy@hornbill.com, provided that if the Customer objects to the changes, it can demonstrate, to Hornbill's reasonable satisfaction, that:

8.12.1. the objection is due to an actual or likely breach of Data Protection Legislation; and
8.12.2. the Customer is acting reasonably and in good faith.

8.13. Hornbill shall use reasonable efforts to address the Customer's objection or recommend a commercially reasonable change to the Customer's use of the Services to avoid Processing of Protected Data by the objected to new Sub-processor. After this process, if a resolution has not been agreed to within 10 business days, Hornbill will proceed with engaging the new Sub-processor and the Customer shall have the right to terminate this agreement in accordance with clause 6.

8.14. Where Hornbill engages Sub-processor for carrying out specific processing activities on behalf of the Customer, materially equivalent data protection obligations as set out herein shall be imposed on that Sub-processor.

8.15. Hornbill shall remain fully liable for all acts or omissions of any Sub-processor, subject to the limitations and exclusions of liability set out herein.

8.16. Subject to clause 4.1 of this agreement, 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.

9. VARIATIONS IN SERVICE PARAMETERS

9.1. Customer may request Hornbill change the Subscription Fee at any time after the Customer Acceptance Date by changing the Service Parameters.

9.2. Hornbill shall produce an interim invoice or voucher, if applicable, to cover the period from the date of the change to the end of the last Subscription Period for which an invoice has been raised. This interim invoice or voucher will be produced as soon as practicable after the change has been made.

9.3. Future invoices will be based upon the revised Subscription Fees until such time as a further change is made.

9.4. The Subscription Fee may not be reduced below that required for the minimum number of Customer Users required on the service being subscribed to.

10. PREVENTION OF FRAUD AND CORRUPTION

10.1. Hornbill shall not offer, give, or agree to give anything, to any person an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the agreement or for showing or refraining from showing favour or disfavour to any person in relation to the agreement.

10.2. Hornbill shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by Hornbill Personnel and Hornbill (including its shareholders, members and directors) in connection with the agreement and shall notify the Customer immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.

10.3. If Hornbill or Hornbill Personnel engage in conduct prohibited by clause 10.1 or commits fraud in relation to the agreement or any other contract with the Customer, the Customer may:

10.3.1. terminate the agreement and recover from Hornbill the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer of making other arrangements for

the supply of the SaaS Service (and Support Service and any other ancillary services) and any additional expenditure incurred by the Customer throughout the remainder of the agreement; or

10.3.2. recover in full from Hornbill any other loss sustained by the Customer in consequence of any breach of this clause.

PARTIES

This agreement is between Hornbill Technologies Limited a company incorporated in England and Wales (registered no. 07244938) whose principal place of business is 3rd Floor, 86-90 Paul Street, London EC2A 4NE ("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 is the provision of a Software-as-a-Service (SaaS) application, through which the Customer and its authorized Users may input, upload, store, or otherwise make available Customer Data for the purposes of operating, managing, or supporting their internal or external business activities. Processing includes all operations performed on such Customer Data as necessary to deliver the functionality of the SaaS Service in accordance with the Customer's use of the application.
Duration of the Processing	Processing will take place until the Termination Date as defined in the Hornbill Subscription Agreement and Hornbill may process the Customer Data after the Termination Date only as required to comply with clauses 6.4.1, 6.4.2 and 8.4.3 of this Agreement.
Nature and purposes of the Processing	The nature of the Processing involves the collection, storage, retrieval, organization, structuring, transmission, analysis, and other operations performed on Customer Data as necessary to deliver, maintain, secure, support, and improve the SaaS Service. The purposes of the Processing are to enable the Customer to use the SaaS Service as intended, including to manage business-related activities, facilitate collaboration, ensure system functionality, generate outputs or reports, and support user interactions. The specific Customer Data processed, and the manner in which it is Processed, is determined and controlled by the Customer through their configuration of the SaaS Service, including the Customer Data they choose to input or make available, the workflows and automations they define, and the features they enable. The Customer acts as the Data Controller and is solely responsible for ensuring that their use of the SaaS Service and Processing of Customer Data complies with applicable laws and aligns with their own internal policies and Processing purposes.

Type of Personal Data	Personal details (including name, address, date of birth, NI number, telephone number) Family, lifestyle and social circumstances Education and training details Employment details Financial details Goods or services provided Racial or ethnic origin Political opinions Trade union membership Physical or mental health or condition Sexual Life Offences (including alleged offences) Criminal proceedings, outcomes and sentences 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 Customer Data Hornbill will Process.

Categories of Data Subject	Staff including temporary and casual workers, volunteers and agents Customers and clients (including prospective) Patients Students / Pupils Members of the Public Users (of a specific service, website etc.) Suppliers Industry Third Parties Relatives, guardians and associates of the data subject Advisers, consultants and other professional experts Partners and Resellers Other (please specify below) I have reviewed the Categories of Data Subject categories above and have checked all those that will be included in the Customer 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 Customer Data once Processing is complete is as set out in the Hornbill Subscription Agreement.

1 Protective Measures - Hornbill Data Security Guide Hornbill Security Policy

1.1 Hornbill Technologies Limited (HTL) is the operating company responsible for hosting the Hornbill SaaS Service and its supporting infrastructure. The Board of Directors and senior management of HTL have established and maintain a robust Information Security Policy, which provides the governance framework through which HTL safeguards the confidentiality, integrity, and availability of all physical and information assets it owns, controls, or processes.

1.2 HTL is certified to ISO/IEC 27001:2022 and ISO/IEC 27018 for its provision and operation of the Hornbill SaaS platform and supporting infrastructure.

1.3 Hornbill Corporate Limited (HCL), the corporate services entity within the Group, is separately certified to ISO/IEC 27001:2022 for its provision of governance, risk, compliance, finance, customer support, development, client services and administrative services to the Hornbill Group.

1.4 Together, these certifications define the scope of Hornbill's ISMS and provide assurance that both operational and corporate information security controls are implemented and maintained effectively. In the following sections unless noted to the contrary references to Hornbill refer to both the HTL and HCL ISMSs.

1.5 Further details of Hornbill's ISMS scope, controls, and certifications are available at: https://trust.hornbill.com/compliance/

2 Information Security

2.1 The Information Security Management Systems (ISMSs) implemented by Hornbill are designed as an enabling framework for the protection of commercially sensitive information and Personal Data processed within both electronic systems and manual filing systems. They aim to safeguard such data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

2.2 Hornbill routinely tests, assesses, and evaluates the effectiveness of its ISMSs, and will update its controls and processes as necessary to respond to emerging security threats, advances in technology, and changes in industry best practices. Any such updates will not materially diminish the commitments, safeguards, or overall levels of service provided to the Customer as described in this agreement.

3 Risk Management

3.1 **Risk Assessment:** Hornbill conducts risk assessments on a continuous and event-driven basis to evaluate both strategic and operational risks. Assessments are initiated whenever material changes occur to any defined Information Asset (as outlined in Section 7), including but not limited to the addition or removal of physical assets, changes to the scope of the ISMSs, modifications to source code, or shifts in the threat landscape.

3.2 **Risk Evaluation Methodology:** Each identified threat-vulnerability pairing is assessed for potential impact using Hornbill's established risk assessment methodology. The impact is evaluated in relation to the value of the affected Asset, and each resulting risk value is recorded within the applicable risk assessment matrix, reflecting confidentiality, integrity, and availability attributes.

3.3 **Vulnerability Management:** Hornbill follows a defined vulnerability management process, under which all hardware and software assets are regularly assessed for vulnerabilities. These assessments leverage trusted industry sources including vendor advisories, the Common Vulnerabilities and Exposures (CVE) database, NIST's National Vulnerability Database (NVD), and internal security testing procedures.

3.4 **Remediation of Critical Vulnerabilities:** All identified critical vulnerabilities are addressed in accordance with Hornbill's current Vulnerability Management Operating Procedure. Remediation is achieved through patching, configuration changes, or compensating controls, and is completed within prescribed timeframes to ensure continued protection of Hornbills infrastructure and services.

4 Management Systems

4.1 Hornbill complies with all applicable national and international data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and, where relevant, the EU GDPR. This commitment applies to all Personal Data Processed by Hornbill, in any format or location, and reflects Hornbill's obligations under ISO/IEC 27001:2022 control A.8.8 (Management of Personally Identifiable Information).

4.2 Personal Data held within Customer Instances is classified as Restricted under HTL's Data Classification Policy and is subject to strict access control measures. Access is granted only on a documented need-to-use and event-specific basis, and solely to authorised Hornbill personnel with a legitimate business requirement. Access rights are regularly reviewed, and all access is logged and auditable in accordance with control A.5.15 (Access Control).

4.3 **Compliance with Security Policies and Standards:** Hornbill maintains a programme of continuous monitoring and review to ensure compliance with its ISMS, in alignment with control A.5.24 (Information Security Policy) and A.5.25 (Information Security Roles and Responsibilities). Regular audits, security reviews, and operational checks are conducted to evaluate the effectiveness of controls and support continual improvement.

4.4 Penetration Testing: To support the ongoing evaluation of system security, Hornbill conducts regular internal vulnerability assessments and contracts with independent third-party security specialists to perform formal penetration testing at least once a year. These tests target the production environment and are designed to identify vulnerabilities and validate the effectiveness of implemented controls, as per control A.8.29 (Security Testing in Development and Acceptance) and A.5.10 (Monitoring, Review and Change Management).

4.5 Identified risks are triaged, remediated or mitigated based on severity and impact, following Hornbill's documented vulnerability management procedures (see also control A.5.4 (Threat Intelligence) and A.8.28 (Vulnerability Management)).

5 Mobile Security

5.1 **Technical Security Measures:** Hornbill enforces strict technical controls for the use of mobile and portable devices in accordance with its ISMSs. These controls apply to laptops, tablets, smartphones, USB storage devices, and other portable computing or storage media. Key requirements include:

5.1.1 Mandatory password or biometric protection on all devices with Two Factor Authentication;

5.1.2 Full-disk encryption applied where technically feasible and appropriate.

5.1.3 Installation of the latest security patches, firmware, and updates for operating systems and applications to address known vulnerabilities.

These measures are aligned with ISO/IEC 27001:2022 controls A.8.1 (User Endpoint Devices) and A.8.9 (Configuration Management).

5.2 **Operational Security Measures:** Hornbill requires the following operational controls to mitigate risks associated with mobile working and user practices:

5.2.1 Notebook computers and portable devices must be always protected against theft and physical damage, including while in use, during transit, and in storage. Any loss or theft must be reported without delay via Hornbill's incident reporting procedures (aligned with control A.5.28).

5.2.2 All users must receive security training appropriate to their role and responsibilities. This training ensures they understand and can fulfil their information security obligations, in accordance with control A.6.3 (Awareness, Education and Training).

6 HR Security

6.1 **Personnel Security:** Hornbill applies pre-employment and ongoing personnel vetting procedures to all individuals, including employees, contractors, agency workers, and

other authorised agents. These procedures are conducted in accordance with Hornbill's documented operating procedures and are subject to applicable local and international laws. Vetting processes are commensurate with the sensitivity of the role and the level of data access granted, in alignment with ISO/IEC 27001:2022 control A.6.1 (Screening).

6.2 **Confidentiality Obligations:** All Hornbill personnel are required to enter into written agreements which include binding confidentiality provisions. These agreements form part of the employment or engagement contract and set out:

6.2.1 The requirement to maintain the confidentiality of all sensitive and personal information;

6.2.2 The limitations on the authorised use of such information;

6.2.3 The personnel's rights and obligations concerning the data;

6.2.4 The actions to be taken upon termination of employment or engagement, including return or secure disposal of information assets.

These measures support ISO 27001:2022 control A.6.2 (Terms and Conditions of Employment) and ensure that Hornbill meets its data protection and confidentiality obligations throughout the employment lifecycle.

7 Asset Management

7.1 **Asset Inventory:** Hornbill maintains a centralised and up-to-date inventory of all information and associated assets relevant to its operations and the ISMS. Each asset within this inventory is uniquely identified, appropriately classified, and assigned an owner.

Assets are categorised under the following classes:

7.1.1 Hardware – Includes all computing and information processing equipment such as servers, laptops, mobile devices, printers, scanners, and multifunction devices;

7.1.2 Software and Information Assets – Includes installed applications, databases, software media, documentation, and digital data repositories;

7.1.3 Services and Facilities – Covers infrastructure and services including networks, cloud platforms, and designated secure physical areas;

7.1.4 People – Refers to individuals whose roles, experience, or knowledge represent critical organisational assets;

7.1.5 Other Assets – Encompasses any remaining tangible or intangible assets that support business operations or information processing activities**.**

This inventory serves as a foundational input to Hornbill's risk assessment and treatment process and is maintained in alignment with ISO/IEC 27001:2022 control A.5.9.

7.2 **Asset Ownership:** Each asset recorded in the inventory has a designated business owner—typically a defined role or department—responsible for:

7.2.1 Ensuring the asset is appropriately classified and protected;

7.2.2 Overseeing the application of security controls relevant to the asset;

7.2.3 Supporting asset lifecycle activities including acquisition, use, monitoring, and secure decommissioning.

Asset owners play a key role in upholding the integrity of the ISMSs by ensuring that their assigned assets are managed in accordance with Hornbill's policies, procedures, and applicable legal or regulatory requirements.

8 Information Classification & Handling

8.1 HTL applies a structured classification scheme to all information assets to ensure they are appropriately protected based on their sensitivity, criticality, and legal or contractual obligations.

HTL classifies information into three distinct levels:

8.1.1 **Restricted** – Information requiring the highest level of protection. This includes Personal Data as defined under applicable Data Protection Legislation (e.g. UK GDPR, EU GDPR). Access is strictly limited to specific individuals or roles, which must be explicitly identified.

8.1.2 **Confidential** – Information that, if disclosed without authorisation, could cause harm to HTL, its customers, or partners. Access is limited to authorised personnel on a need-to-know basis.

8.1.3 **Public** – Information approved for public dissemination with no significant confidentiality risks.

Information classified as Restricted, including all Personal Data, is subject to additional controls and handling procedures as set out in HTL's Information Classification and Handling Operating Procedure.

These classification levels support the correct labelling, access control, transmission, and retention of information in accordance with ISO 27001 best practices.

8.2 HCL applies a structured classification scheme to all information assets to ensure they are appropriately protected based on their sensitivity, criticality, and legal or contractual obligations.

HCL classifies information into two distinct levels:

8.2.1 **Restricted** – Information requiring the highest level of protection. This includes:

8.2.1.1 Personal Data as defined under applicable Data Protection Legislation (e.g. UK GDPR, EU GDPR)

8.2.1.2 Security Credentials

8.2.1.3 Hornbill / SupportWorks related data

8.2.1.4 Data in our internal instance of hornbill

8.2.1.5 Source Code / Intellectual Property

8.2.1.6 Human Resources data

Access is strictly limited to specific individuals or roles, which must be explicitly identified.

8.3 **Not Restricted** –Not Restricted Assets may be shared freely internally, wherever possible we should only share them with those who need to access them. Not Restricted Assets should only be shared externally if we are confident that the risk should they be passed on to other third parties (either intentionally or as a result of hacking) falls into either of the categories where no harm arises, or the disclosure only causes minor reputational damage or minor operational impact.

These classification levels support the correct labelling, access control, transmission, and retention of information in accordance with ISO 27001 best practices.

9 Access Control

9.1 **Access Management to Instances:** HTL ensures that access to the SaaS Service by authorised HTL personnel and approved Sub-processors is secured and governed through robust authentication, authorisation, and segregation controls. Access rights are granted on a strict *need-to-use* and *event-specific* basis.

Access provisioning and deprovisioning are handled via formal registration and deregistration procedures under the supervision of the HTL ISMS Manager. All access privileges are recorded and routinely audited to confirm that:

9.1.1 Access rights have been revoked in accordance with termination or role change requests;

9.1.2 Privileges remain appropriate, valid, and proportionate to the individual's responsibilities;

9.1.3 No unauthorised access rights have been granted.

User access rights are promptly reviewed following personnel role changes, ensuring continued alignment with data protection and least-privilege principles, in line with ISO/IEC 27001:2022 controls A.5.16 and A.5.17.

9.2 **Technical and Network Access Control:** Hornbill applies multiple layers of technical and network access controls to protect its service infrastructure, including but not limited to:

9.2.1 Secure log-on mechanisms and enforced authentication policies;

9.2.2 Network access controls via VPNs and firewalls with strict port management;

9.2.3 Logical network segmentation with defined inter-network routing and connection protocols;

9.2.4 Continuous real-time monitoring and logging of access attempts, system events, and data flows;

9.2.5 Automated log analysis for anomalies or threats, with corrective actions promptly applied (e.g., blocking automated scanners or suspicious IP addresses).

These controls support compliance with ISO 27001:2022 controls A.5.15, A.8.15, A.8.16, and A.8.17.

9.3 **Service-Level Access Controls:** HTL's SaaS platform provides configurable, granular access controls based on roles and user privileges. The Customer is solely responsible for configuring, managing, and maintaining access controls within their designated HTL instance.

Each user must be assigned secure authentication credentials and an appropriate role to enforce the principle of least privilege. The Customer is responsible for the confidentiality and proper assignment of these credentials to maintain secure access to the SaaS Service.

In addition to the above Hornbill implements a comprehensive suite of access control measures to safeguard information systems and data, aligned with ISO/IEC 27001:2022 controls A.5.15 to A.5.18 and A.8.15 to A.8.17.

9.4 **User Access Management**

9.4.1 **Controlled Access Lifecycle:** Formal processes are in place for user registration, de-registration, and access change requests. Access rights are revoked upon termination or role change.

9.4.2 **Least Privilege Principle:** Access is granted strictly based on job responsibilities, minimising unnecessary permissions.

9.4.3 **Regular Reviews:** User access rights are periodically reviewed to ensure ongoing appropriateness.

9.4.4 **Segregation of Duties:** Conflicting responsibilities are separated to reduce the risk of fraud or bypass of controls.

9.4.5 **Unique User IDs:** Each user is assigned a unique identity, managed throughout its lifecycle for traceability and access assignment.

9.5 **Authentication and Password Security**

9.5.1 **Strong Authentication:** Multi-factor authentication is enforced. Hardware tokens or biometrics are preferred over passwords where possible.

9.5.2 **Password Policy Compliance:** All credentials must meet defined complexity and management requirements in line with Hornbill's Password Policy.

9.6 **System and Application Access Controls**

9.6.1 **Network and OS Protections:** Access to network services, systems, and operating environments is restricted through layered security mechanisms.

9.6.2 **Role-Based Access:** Application and information access is governed by user roles to ensure least privilege and prevent unauthorised data exposure.

9.7 **Access Monitoring and Auditing**

9.7.1 **Active Monitoring:** All user access is logged and monitored to detect anomalies or unauthorised activity.

9.7.2 **Audit and Compliance Reviews:** Regular audits are conducted to verify adherence to access control policies and the effectiveness of technical safeguards.

10 **Cryptography Controls and Usage**

10.1 **Data in Transit and Backup Encryption:** Hornbill ensures that all data transmitted over networks is protected using strong, industry-standard encryption protocols, including Transport Layer Security (TLS). All data in motion is encrypted via HTTPS/SSL, safeguarding it against unauthorised interception or tampering during transmission.

In accordance with ISO/IEC 27001:2022 Control A.8.24 (Use of Cryptography), all system and service backups are encrypted to protect the confidentiality and integrity of customer data throughout the backup lifecycle.

10.2 **Data at Rest Encryption:** HTL provides full encryption at rest using Advanced Encryption Standard (AES-256) for all customer SaaS instances. This ensures that stored data remains protected against unauthorised access, even in the event of physical compromise. Where applicable, specific sensitive data fields may be additionally encrypted based on classification and risk level.

These encryption measures align with ISO/IEC 27001:2022:

10.2.1 A.8.24 – Use of Cryptography: ensuring the confidentiality, integrity, and (where required) authenticity of information;

10.2.2 A.8.25 – Key Management: supporting the secure management of encryption keys and cryptographic materials.

HTL's encryption strategy is an integral part of its broader Information Security Management System (ISMS), designed to meet customer, regulatory, and contractual requirements.

11 **Physical and Environment Security**

11.1 **Data Centre Facilities:** HTL delivers its SaaS Service from geographically designated data centres located within the Customer's selected Hosting Zone, ensuring compliance with applicable data protection regulations. All data centres are independently certified to ISO/IEC 27001 and SSAE-16/ISAE 3402 standards, supporting high assurance levels for information security, availability, and confidentiality.

Hornbill hosts servers and remote desktop workstations from data centres ensuring compliance with applicable data protection regulations. All data centres are independently certified to ISO/IEC 27001 and SSAE-16/ISAE 3402 standards, supporting high assurance levels for information security, availability, and confidentiality.

11.2 **Physical Security Controls at Data Centres:** Hornbill's hosting partners implement multi-layered physical security controls, including but not limited to:

11.2.1 External and internal CCTV surveillance;

11.2.2 Biometric and proximity card access systems;

11.2.3 Dual-authentication entry with mantraps;

11.2.4 Intrusion detection and door tamper alarms;

11.2.5 24/7 on-site security personnel;

11.2.6 Perimeter protection (e.g. secure fencing, gated access);

11.2.7 Controlled access loading docks for secure deliveries;

11.2.8 Fire detection and suppression systems across all critical areas.

These measures align with ISO/IEC 27001:2022 controls A.7.1–A.7.4, A.7.10–A.7.11, ensuring only authorised personnel can access physical infrastructure and assets.

11.3 **Office Facilities:** Hornbill's office environments are subject to appropriate physical and environmental controls in accordance with the Hornbill Corporate ISMS. Measures include:

11.3.1 Secure access control using electronic passes or controlled keys and visitor registration;

11.3.2 Alarmed entry points and monitored CCTV coverage in sensitive areas;

11.3.3 Secure workspaces for personnel processing sensitive data or performing privileged functions;

11.3.4 Locked storage for confidential documentation and portable media;

11.3.5 Clear desk and screen policies in all shared or multi-use spaces.

These office facility controls are aligned with ISO/IEC 27001:2022 control A.7.5 (Physical Entry Controls) and A.7.9 (Clear Desk and Screen Policy) to protect business-critical operations and Personal Data.

11.4 **Secure Management and Disposal of Equipment:** Hornbill ensures the secure disposal of information processing assets, including storage media and hardware. Disposal processes are executed in accordance with ISO/IEC 27001:2022 control A.8.11 (Data Deletion) and A.8.12 (Disposal of Equipment), and include:

11.4.1 Physical destruction of decommissioned or damaged hard drives containing Personal Data;

11.4.2 Sanitisation of storage media using approved data-wiping methods;

11.4.3 Disposal via licensed contractors in full compliance with the UK WEEE Regulations (or regional equivalent), ensuring environmentally responsible and secure handling of obsolete equipment.

12 Operations

12.1 **Capacity Management:** Hornbill Technologies Limited (HTL) implements proactive capacity management to ensure the SaaS Service remains scalable, resilient, and responsive to both current and anticipated customer demands. System components including network bandwidth, CPU usage, memory, disk utilisation, and load are continuously monitored, with automated alerting to pre-empt performance degradation or resource exhaustion.

These practices are aligned with ISO/IEC 27001:2022 control A.8.5, supporting the ongoing availability and efficiency of service delivery.

12.2 **Monitoring and Telemetry:** Each HTL customer instance is monitored in real time from multiple geographically dispersed locations. Monitoring is conducted at five-minute intervals across more than 100 system metrics, covering:

12.2.1 Performance: DNS propagation, ping times, API response times, CPU load, RAM load, disk I/O, and network throughput;

12.2.2 Hardware Health: Availability, temperature, SMART monitoring, and SNMP status;

12.2.3 Capacity: Resource usage including disk space, CPU, memory, and input/output performance;

12.2.4 Availability: Service uptime checks via ping, DNS queries, API endpoint testing, and host controller verification;

12.2.5 Security & Intrusion Detection: Continuous log file analysis, traffic pattern recognition, packet and bandwidth anomaly detection, and intrusion detection system (IDS) alerts;

12.2.6 Data Leakage Detection: Real-time monitoring for signs of unauthorised data exfiltration using bandwidth/source/destination traffic analysis;

12.2.7 Backup Integrity: Sync and replication status, off-instance availability, and consistency verification;

12.2.8 Sanity Checks: Queue lengths, system load validations, and service-specific readiness tests.

These controls support compliance with ISO/IEC 27001:2022 controls A.8.15–A.8.17, ensuring effective system monitoring, logging, and alerting to maintain service integrity and early threat detection.

13 Supplier Relationships and Procurement

13.1 HTL conducts formal risk assessments prior to granting system or data access to any third parties, including customers, in accordance with the current published operating procedures and aligned with its ISMS.

In accordance with ISO/IEC 27001:2022 control A.5.4 (Threat Intelligence) and A.5.19–A.5.21 (Supplier Relationships), the assessment process evaluates the following risk factors:

13.1.1 **Physical Access Risks** – Including access to HTL-managed premises, data centres, or secure areas;

13.1.2 **Logical Access Risks** – Including access to HTL networks, systems, APIs, or data repositories;

13.1.3 **Legal, Regulatory, and Contractual Obligations** – Including compliance with data protection laws (e.g. GDPR), export controls, industry-specific standards, and customer contractual terms.

Where access is granted, HTL defines the required technical and organisational controls to be implemented by the external party. These control requirements are clearly documented and agreed upon within a legally binding contract, data processing agreement, or service-level agreement (SLA), in accordance with ISO/IEC 27001:2022 controls A.5.22 (Managing Information Security in Supplier Relationships) and A.5.23 (Monitoring and Review of Supplier Services).

HTL retains responsibility for ensuring that access by third parties is subject to ongoing risk monitoring and audit as part of its ISMS governance framework.

13.2 Hornbill implements a risk-driven and contractually governed supplier management process, aligned with **ISO/IEC 27001:2022 controls A.5.19 to A.5.23**, to ensure the security and integrity of its supply chain.

13.2.1 **Supplier Selection and Risk Assessment**

13.2.1.1 **Risk-Based Evaluation**: All suppliers are subject to formal risk assessments based on the sensitivity of data handled and the criticality of services provided.

13.2.1.2 **Due Diligence**: Security due diligence includes review of supplier policies, certifications (e.g., ISO 27001), and, where appropriate, site assessments.

13.2.1.3 **Approval Requirement**: Supplier onboarding requires formal management approval based on risk assessment outcomes.

13.2.2 **Contractual Safeguards**

13.2.2.1 **Security Clauses**: All supplier contracts include mandatory information security provisions covering data handling, access control, incident reporting, and policy compliance.

13.2.2.2 **Confidentiality Agreements**: Suppliers must sign NDAs to safeguard Hornbill's sensitive information.

13.2.2.3 **Right to Audit**: Contracts provide Hornbill with the right to audit supplier compliance with agreed security obligations.

13.2.3 **Ongoing Supplier Management**

13.2.3.1 **Continuous Monitoring**: Supplier performance and security practices are regularly assessed through audits, meetings, and review of compliance reports.

13.2.3.2 **Performance Reviews**: Formal performance reviews are conducted to ensure alignment with contractual security requirements.

13.2.3.3 **Incident Reporting Obligations**: Suppliers must report information security incidents immediately and cooperate with any investigations or remediation activities.

13.2.4 **Secure Termination Procedures**

13.2.4.1 **Access Revocation and Data Return**: Upon contract termination, all access to Hornbill systems is revoked, and any data held by the supplier must be returned or securely destroyed.

13.2.4.2 **Exit Review**: A formal review ensures all contractual and security obligations are fulfilled, and residual risks are mitigated.

13.2.5 **Compliance and Policy Governance**

13.2.5.1 **Audit and Oversight**: Supplier compliance is monitored through periodic audits and assessments.

13.2.5.2 **Issue Reporting**: Any supplier-related security risks must be reported immediately to senior management.

13.2.5.3 **Policy Maintenance**: The supplier management policy is reviewed annually, incorporating audit feedback, incident learnings, and regulatory changes for continuous improvement.

14 Incident Reporting\Handling and Management

14.1 **Incident Reporting and Handling:** Hornbill maintains a formalised incident management process to ensure timely detection, reporting, classification, and response to all information security incidents. All suspected or actual incidents are immediately escalated to the Information Security Manager, who is responsible for:

14.1.1 Performing a preliminary assessment of the incident;

14.1.2 Categorising the incident based on severity and impact;

14.1.3 Coordinating response and remediation activities in line with documented HTL operating procedures.

These practices are aligned with ISO/IEC 27001:2022 controls A.5.28 and A.5.29, ensuring incidents are managed efficiently and consistently.

14.2 **Notification of Personal Data Breaches:** In the event that Hornbill becomes aware of any unauthorised access to, alteration, disclosure, accidental or unlawful destruction, or loss of Personal Data (a “Breach”), Hornbill will notify the Customer or relevant party without undue delay, and in accordance with Clause 8.5 of this Agreement and applicable data protection laws (e.g. UK GDPR, EU GDPR). This obligation supports compliance with ISO/IEC 27001:2022 control A.5.29, as well as data breach notification requirements under relevant legislation.

14.3 **Customer Notification and Ongoing Updates:** Initial breach notifications will be made to the Customer’s designated authorised contact(s) for the affected Hornbill instance. As the investigation progresses and additional information becomes available, Hornbill will continue to provide timely updates, unless restricted by applicable law or legal obligation.

Updates may include:

14.3.1 Nature, scope, and root cause of the breach;

14.3.2 Categories and volume of Personal Data affected;

14.3.3 Remediation actions taken or planned;

14.3.4 Support information to enable the Customer to fulfil its obligations to inform affected Data Subjects, supervisory authorities, or other relevant third parties in accordance with applicable Data Protection Legislation.

15 Change Reporting\Handling\Planning and Management

15.1 Change Management: Hornbill maintains a formal change management process to ensure that modifications to systems, services, or infrastructure are properly assessed, authorised, and implemented without introducing unacceptable risk.

All proposed changes must be authorised by a suitable qualified person, in consultation with relevant stakeholders. Changes are not approved for implementation until the following conditions are met:

15.1.1 A documented risk assessment is completed to evaluate potential impacts;

15.1.2 Where applicable, fallback procedures or a rollback strategy are prepared to restore service in the event of failure;

15.1.3 For significant or high-risk changes, a comprehensive testing plan is created, including:

15.1.3.1 Business, technical, and load acceptance criteria;

15.1.3.2 Evidence of a successful dry run or simulation where feasible.

These controls are in alignment with ISO/IEC 27001:2022 control A.8.32, ensuring changes are managed in a structured and traceable manner to protect the integrity of services and information.

15.2 Promotion to Production Environment: All functional and non-functional testing is conducted within a dedicated, logically separated test environment configured specifically for the proposed change. Production and test environments are segregated to prevent unauthorised impact on operational services.

15.3 Following successful completion of testing and validation against the defined acceptance criteria, the HTL Cloud Service Manager authorises the deployment of the change into the production environment. This step ensures:

15.3.1 Business continuity is preserved, with no unintended disruption to services;

15.3.2 Any required updates to business continuity plans or related documentation are completed in accordance with operational risk procedures.

These practices also support compliance with ISO/IEC 27001:2022 control A.8.9 (Configuration Management) by maintaining the integrity and traceability of deployed changes.

16 Business Continuity and Disaster Recovery

16.1 Business Continuity Planning: Hornbill is committed to maintaining customer access to the SaaS Service and associated data, even in the event of a major disruption, emergency, or disaster.

Hornbill's Business Continuity and Disaster Recovery (BC/DR) plans are designed to ensure service restoration within minimal downtime. In the event of a critical failure affecting a primary data centre, the SaaS Service will be restored from a secondary data centre with the objective of minimising customer impact and achieving rapid recovery time objectives (RTOs).

These provisions are aligned with ISO/IEC 27001:2022 controls A.5.31 and A.5.32, supporting continuity of critical information security and ICT services during adverse events.

16.2 **Backup and Data Replication:** Hornbill employs a multi-tiered backup and replication strategy to ensure data integrity, availability, and recoverability:

16.2.1 Real-Time Replication: All SaaS-related databases are synchronised in real time to a geographically separated secondary data centre.

16.2.2 File Replication: File systems are replicated every five minutes to ensure near-continuous protection.

16.2.3 Daily Encrypted Backups: All replicated data is backed up daily to a tertiary location within the customer's contracted hosting region. Each backup is stored as a secure, encrypted archive protected by a single-use key.

Backup processes are non-disruptive and operate without impacting service availability. These controls conform to ISO/IEC 27001:2022 control A.8.13 (Backup) and ensure both operational resilience and compliance with data protection obligations.