hyperproof

MAIN SUBSCRIPTION AGREEMENT

This Main Subscription Agreement (the "**Agreement**") is made by and between Hyperproof, Inc., a Delaware corporation headquartered at 600 1st Ave Ste 330, PMB 78059 Seattle, Washington 98104 ("**Hyperproof**") and the entity accepting this Agreement by signing below ("**Customer**"). The Agreement is effective between Customer and Hyperproof as of the date of Customer accepting it ("**Effective Date**"). "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. Control means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity. The "**Services**" means the products that are ordered by Customer under an Order Form and made available by Hyperproof. "**User**" means an individual who is authorized by Customer to use a Service, for whom Customer has purchased a subscription (or for whom a Service has been provisioned), and to whom Customer has supplied user identification and authentication. "**Program**" means an instantiated compliance framework authorized by Customer to use within the Service, for whom Customer has purchased a subscription (or for whom a Service has been provisioned). "**Module**" means an additional Hyperproof component authorized by Customer to use within the Service, for whom Customer has purchased a subscription (or for whom a Service has been provisioned).

1. COMMERCIALS

1.1 Fees, Invoicing, and Payment. The "**Fees**" means the fees, expenses, and other amounts specified in this Agreement and applicable Order Form. "**Order Form**" means the ordering document specifying Services to be provided hereunder that is entered into between Customer and Hyperproof. By entering into an Order Form, an Affiliate agrees to be bound by this Agreement as if it were an original party hereto. All amounts payable are: (i) denominated and payable in United States Dollars, (ii) payment obligations are non-cancelable and fees paid are non-refundable, and (iii) quantities purchased cannot be decreased during the relevant subscription term. The Fees listed in the Order Form will be fixed for the term listed in the Order. Except as otherwise set forth in the applicable Order Form (a) fees are payable in advance; (b) Customer shall pay invoices within thirty (30) days after receipt of electronic invoice; and (c) payment shall be made by ACH or wire transfer to the bank account designated by Hyperproof or by check to the address in the Order Form.

1.2 Subscriptions and True up. Unless otherwise provided in the applicable Order Form, (a) Services are purchased as subscriptions for the term stated in the applicable Order Form, (b) subscriptions for a Service may be added during a subscription term at the same pricing as the underlying subscription pricing for that Service, prorated for the portion of that subscription term remaining at the time the subscriptions are added, and (c) any added subscriptions will terminate on the same date as the underlying subscriptions. Customer agrees that its purchases are not contingent on any future functionality or features, or dependent on any oral or written public comments made by Hyperproof regarding future functionality or features. If Customer's Program / Module count exceeds the current number of subscriptions (determined on a monthly basis), then Hyperproof will notify Customer (email sufficing) of such overage. If Customer does not reduce the number of actual Programs / Modules to the authorized number within 30 days, Hyperproof will invoice Customer for the excess Programs / Modules (who will then become additional authorized Programs / Modules), prorated for the remainder of the then-current subscription term. If Hyperproof provides Customer with access to the Service in advance

of the start date specified in the applicable Order Form, Customer's use during that period will be governed by the terms of this Agreement, and the license restrictions set forth herein.

1.3 **Professional Services.** Additional support services, including custom configuration, consulting, training and system integration, may be separately purchased from Hyperproof under the terms of an Order Form, work order or statement of work referencing this Agreement. For clarity, Hyperproof has no obligation to support Customer's own technology, internal infrastructure, provide free training, or provide consulting on customer created content or third-party technologies and services unless agreed to in writing via an approved Order Form, work order or statement of work.

1.4 **Term.** This Agreement commences on the Effective Date and continues until all subscriptions hereunder have expired or have been terminated. Each subscription term is specified in the applicable Order Form. Each Order Form will specify whether the applicable subscription will automatically renew or expire at the end of the subscription term, and if not specified, the subscription will expire.

1.5 **Termination**. A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. If this Agreement is terminated by Customer in accordance with this section, Hyperproof will refund Customer any prepaid fees covering the remainder of the term of all Order Forms after the effective date of termination. Upon expiration or termination of the subscription term or applicable Order Form, access to the Services will terminate and Customer will immediately cease accessing and using the Services.

1.6 **Taxes**. Fees do not include any taxes, levies, duties or similar governmental assessments, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction ("**Taxes**"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If Hyperproof has the legal obligation to pay or collect Taxes for which Customer is responsible under this section, Hyperproof will invoice Customer and Customer will pay that amount unless Customer provides Hyperproof with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, Hyperproof is solely responsible for taxes assessable against it based on its income, property, and employees.

2. PARTY RESPONSIBILITIES, INTELLECTUAL PROPERTY, AND CONFIDENTIALITY

2.1 **Hyperproof Provision of Services**. Hyperproof will (a) make the Services available to Customer subject to this Agreement, including the attached Service Level Addendum, and the applicable Order Forms, and (c) provide the Services in accordance with laws and government regulations applicable to Hyperproof's provision of its Services to its customers generally (i.e., without regard for Customer's particular use of the Services). Hyperproof will be responsible for the performance of its personnel (including its employees and contractors) and their compliance with Hyperproof's obligations under this Agreement.

2.2 **Hyperproof Protection of Customer Data**. Hyperproof will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data.

"**Customer Data**" means electronic data and information submitted by or for Customer to the Services. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users). The terms of the data processing addendum ("**DPA**") published by Hyperproof contained herein is hereby incorporated and will apply to the extent Customer Data includes Personal Data, as defined in the DPA. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by Hyperproof, the Standard Contractual Clauses will apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and any applicable execution of an Order Form by Company or an Affiliate, will be treated as its execution of the Standard Contractual Clauses and related Appendices.

2.3 **Customer Compliance**. Customer will (a) be responsible for its Users' compliance with this Agreement and Order Forms, (b) be responsible for the accuracy, quality, and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Services, (c) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Hyperproof promptly of any such unauthorized access or use, and (d) use the Services only in accordance with this Agreement, Order Forms, and applicable laws and government regulations. If Customer breaches its payment obligations, Hyperproof may suspend delivery of the Services after providing 30 days' notice (including by phone or email) in the event such breach remains uncured at the end of such period.

2.4 **Reservation of Intellectual Property Rights**. Subject to the limited rights expressly granted hereunder, Hyperproof and its licensors reserve their right, title, and interest in and to the Services, including all of their related intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

2.5 **License by Customer to Hyperproof**. License by Customer to Hyperproof. Customer grants Hyperproof a license to host, copy, use, transmit, and display any Customer Data and program code created by or for Customer for the sole purpose of providing Customer with service under this Agreement. Subject to the limited licenses granted herein, Hyperproof acquires no right, title, or interest from Customer or its licensors under this Agreement in or to any Customer Data or such program code.

2.6 **IP Infringement**. If Hyperproof receives information about an infringement or misappropriation claim related to a Service, Hyperproof may in its discretion and at no cost to Customer (i) modify the Services so that they are no longer claimed to infringe or misappropriate, without breaching Hyperproof's warranties under "**Hyperproof Warranties**" below, (ii) obtain a license for Customer's continued use of that Service in accordance with this Agreement, or (iii) terminate Customer's subscriptions for that Service upon 30 days' written notice and refund Customer any prepaid fees covering the remainder of the term of the terminated subscriptions.

2.7 **Confidential Information**. "**Confidential Information**" means all information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the

information and the circumstances of disclosure. Confidential Information of Customer includes Customer Data; Confidential Information of Hyperproof includes the Services, the terms and conditions of this Agreement, and all Order Forms (including pricing). Confidential Information of each party includes technology and technical information, product plans, and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

2.8 **Protection of Confidential Information**. Each party retains all ownership rights in and to its Confidential Information. The Receiving Party will use the same degree of care it uses to protect its own confidential information of like kind to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors, and sub contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party that are not materially less protective than those herein. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel, and accountants without the other party's prior written consent, provided that such Disclosing Party remains responsible for its Affiliates, legal counsel, and accountants' compliance with this section. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law, provided the Receiving Party gives the Disclosing Party prior notice (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling.

3. REPRESENTATIONS, WARRANTIES, AND DISCLAIMERS

3.1 **Representations and Warranties**. Each Party represents that it has validly entered into this Agreement and has the legal power to do so. This Agreement and the Documentation accurately describes the administrative, physical, and technical safeguards for protecting the security, confidentiality, and integrity of Customer Data, and Hyperproof warrants, during an applicable subscription term, that: (a) Hyperproof will not materially decrease the overall security of the Services; (b) the Services will perform materially in accordance with the applicable Documentation; and (c) Hyperproof will not materially decrease the overall functionality of the Services. For any breach of a warranty above, Customer's exclusive remedies are set forth in the "**Termination**" section.

3.2 **Disclaimers.** EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY LAW.

4. MUTUAL INDEMNIFICATION

4.1 Indemnification. Hyperproof will defend the Customer against any claim, demand, suit or proceeding made or brought against the Customer by a third party alleging (i) that the Services provided by Hyperproof infringes or misappropriates such third party's intellectual property rights; (ii) Hyperproof's gross negligence, intentional misconduct or violation of applicable law (a "Claim"), and will indemnify the Customer from any damages, attorney fees, and costs finally awarded against theCustomer as a result of, or for amounts paid by, the Customer under a settlement approved by Hyperproof in writing of, a Claim, provided that the Customer: (a) promptly gives Hyperproof written notice of the Claim; (b) gives Hyperproof sole control of the defense and settlement of the Claim (except that Hyperproof may not settle any Claim unless it unconditionally releases the Customer of all liability); and (c) gives Hyperproof all reasonable assistance, at Hyperproof's expense.

4.2 Indemnification Exceptions. The defense and indemnification obligations in Section 4.1 do not apply if the Claim arises: (1) from Customer's use or combination of the Services with software, hardware, data, or processes that are not provided by Hyperproof or authorized by Hyperproof in writing, if the Services or use thereof would not infringe without such combination; (2) in whole or in part from the Indemnified Party's breach of this Agreement or Order Forms; (3) from Customer's modification or alteration of the Services in a manner not authorized by Hyperproof in writing, if the Services would not infringe without such modification or alteration; or (4) from the Indemnified Party's own malfeasance.

5. LIMITATION OF LIABILITY

5.1 Limitation of Liability. A PARTY AND ITS AFFILIATES' AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY CUSTOMER AND ITS AFFILIATES HEREUNDER IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE ANY LIABILITY LIMIT. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "FEES, INVOICING, AND PAYMENT" SECTION.

5.2 Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

5.3 Excluded Claims. Section 5.1 does not apply to claims arising under Section 1.1 (Fees, Invoicing, and Payment), Section 4.1 (Indemnification, confidentiality obligations, or with respect to a violation by one party of the other party's intellectual property rights), and Section 2.4 (Reservation of Intellectual Property Rights).

5.4 Data Protection Limitation. Specifically with respect to Hyperproof's obligations of confidentiality or data security, in no event will Hyperproof's or its Affiliates' liability arising out of or related to this

Agreement exceed two times (2x) the amounts paid or payable by the customer and its Affiliates hereunder in the twelve months preceding the first incident out of which the liability arose.

6. CORE OPERATIONAL TERMS

6.1 Usage Data. Hyperproof may store and use metadata associated with Customer's use of the Services, including but not limited to IP addresses, stored sessions, and network metadata (collectively, "Customer Metadata") for the purpose of providing the Services to Customer. In addition, Hyperproof may track and analyze the usage of the Services for purposes of security and helping Hyperproof improve both the Services and the user experience in using the Services. For example, to improve product functionality we may use this information to understand and analyze trends or track which features are used most often. Hyperproof may aggregate Customer Data and Customer Metadata with data and metadata from other Hyperproof customers or other sources, provided that such data and metadata is not identifiable as Customer Data or Customer Metadata and Customer cannot be recognized as its source. Hyperproof may share anonymous usage data with Hyperproof's service providers for the purpose of helping Hyperproof in such tracking, analysis, and improvements. Additionally, Hyperproof may share such anonymous usage data on an aggregate basis in the normal course of operating our business.

6.2 Feedback. Customer grants to Hyperproof and its Affiliates a worldwide, perpetual, irrevocable, royalty free license to use and incorporate into its services any suggestion, enhancement request, recommendation, correction, or other feedback provided by Customer or Users relating to the operation or use of the Services. Hyperproof acknowledges that Customer provides all feedback and suggestions "as is," and that Customer makes no representation or warranty, express or implied, as to the accuracy, noninfringement, or completeness thereof.

6.3 Customer Usage Restrictions. Customer will not (a) make the Services available to anyone other than Customer or its Users, or use the Services for the benefit of anyone other than Customer or its Affiliates, (b) sell, resell, license, sublicense, distribute, make available, rent or lease the Services, or include the Services in a service bureau or outsourcing offering, (c) interfere with or disrupt the integrity or performance of the Services, (d) attempt to gain unauthorized access to the Services or related systems or networks, (e) use the Services to access or use any of Hyperproof intellectual property except as permitted under this Agreement, (f) modify, copy, or create derivative works based on the Services or any part, feature, function, or user interface thereof, (i) frame or mirror any part of the Services, other than framing on Customer's own intranets or otherwise for its own internal business purposes, (g) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Services or access it to (1) build a competitive product or service, (2) build a product or service using similar ideas, features, functions or graphics of the Services, or (3) copy any ideas, features, functions or graphics of the Services; or (h) upload or provide Hyperproof with any personally identifiable information or other Customer Data to which Customer does not have all rights and permissions necessary to provide to Hyperproof for use as permitted in this Agreement.

6.4 **Return and Deletion of Customer Data**. Hyperproof will make the Customer Data available for up to 30 days after the Agreement ends to enable the customer to extract the data. After such 30-day period, Hyperproof will have no obligation to maintain or provide any Customer Data.

6.5 **Documentation**. Hyperproof's online help FAQs, user guides, training manuals and similar product documentation of the Services are available for review at https://docs.hyperproof.io/, as updated or revised by Hyperproof from time to time (the "**Documentation**").

7. GENERAL PROVISIONS

7.1 **Assignment**. Neither party may assign any of its rights or obligations in this Agreement without the other party's prior written consent (not to be unreasonably withheld); provided, however, either party may assign this Agreement (including all Order Forms), without the other party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all assets; provided, however, if a party is acquired by, sells substantially all its assets to, or undergoes a change of control in favor of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice. In the event of such a termination, Hyperproof will refund any prepaid Fees covering the remainder of the term of all subscriptions for the period after the effective date of such termination.

7.2 **Relationship of the Parties and Third-Party Beneficiaries**. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. Each party will be solely responsible for payment of all compensation owed to its employees, as well as all employment-related taxes. There are no third-party beneficiaries under this Agreement.

7.3 **Surviving Provisions**. The sections titled "Fees, Invoicing, and Payment," "Reservation of Intellectual Property Rights," "Protection of Confidential Information," "Disclaimers," "Mutual Indemnification," "Limitation of Liability," "Core Platform Operational Terms," and "General Provisions" will survive any termination or expiration of this Agreement, and the section titled "Protection of Customer Data" will survive any termination or expiration for so long as Hyperproof retains possession of Customer Data.

7.4 **Export Compliance and Anti-Corruption**. The Services may be subject to export laws and regulations of the United States and other jurisdictions. Hyperproof and Customer each represent that it is not named on any U.S. government denied-party list. Customer will not permit any User to access or use any Service in a U.S. embargoed country or region or in violation of any U.S. export law or regulation. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement.

7.5 **Force Majeure**. Neither Party will be in breach due to any delay or failure to perform resulting from any cause or condition beyond such Party's reasonable control. If a force majeure event delays or prevents Hyperproof's performance, the Fees will be equitably adjusted. The Party seeking relief from performance must (i) provide notice of the circumstances as soon as practicable; (ii) use commercially reasonable efforts to avoid or mitigate them; and (iii) resume performance as soon as practicable. If the

failure or delay continues for more than 30 days, then the other Party may terminate this Agreement without liability, except that, if Customer terminates this Agreement for Hyperproof's failure, Hyperproof shall provide a prorated refund for any prepaid Fees for the remaining portion of the subscription term for the Services. This section will not apply to any accrued payment obligations.

7.6 **Governing Law and Notices**. This Agreement is governed by the laws of the state of Delaware, USA, without regard to conflict-of-laws principles. The parties agree that in the event of any action arising out of this Agreement, the parties consent to personal jurisdiction and the exclusive venue in the state and federal courts located in Delaware. Except as otherwise specified in this Agreement, all notices related to this Agreement will be in writing and will be effective upon (a) personal delivery, (b) the second business day after mailing, to the parties at the address in the applicable Order Form or (c), except for notices of termination, dispute, lawsuit, or an indemnifiable claim ("Legal Notices"), which shall clearly be identifiable as Legal Notices, the day of sending by email: to Hyperproof at legal@Hyperproof.io or to Customer at the email provided in the Order Form.

7.7 **Entire Agreement, Order of Precedence, Waiver, and Severability**. This Agreement is the entire agreement between Hyperproof and Customer regarding Customer's use of Services and supersedes all prior and contemporaneous agreements, proposals, or representations (written or oral) concerning its subject matter, including without limitation, any NDA or confidentiality agreement entered into by the parties prior to the execution of this Agreement. Any term or condition stated in any other Customer order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be the: (1) applicable Order Form, (2) Agreement. Titles and headings of sections of this Agreement are for convenience only. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

Customer	Hyperproof, Incorporated
Signature:	**Signature**:
Name:	**Name**:
Title:	**Title**:
Date:	**Date**:

SERVICE LEVEL ADDENDUM

This Service Level Addendum is part of the Agreement between Hyperproof and Customer.

1) **Customer Support**. Hyperproof customer support center is available 24 hours a day, 7 days a week. Customer may reach Hyperproof customer support through the Hyperproof support web site or by email to support@hyperproof.io. Customer must designate a maximum of two support delegates. Support delegates are the designated persons for Hyperproof to contact when Customer's input is required to resolve an issue. Alternatively, instead of designating individual support delegates, Customer may create an email alias (such as "Hyperproofsupport@[customer].com") for Hyperproof to send support delegate emails.

2) **Response Time**. Hyperproof will respond to Customer support inquiries during regular business hours according to Customer's support entitlements as set forth in the Order Form. Standard support customers are entitled to service from 9:00 AM to 5:00 PM Monday - Friday in the single timezone they select from the available timezones ("Standard Support"). If selected by Customer in the Order Form, Premium support customers are entitled to service from 9:00 AM to 5:00 PM Monday - Friday in all of the available timezones ("Premium Support"). Available timezones: CET, GMT, EST, CST, MST, PST. Service is available in accordance with the following response time schedule provided that the user submits a support ticket via Hyperproof's support web site or support@hyperproof.io.

Priority	Description	Standard Support Target Initial Response Time	Premium Support Target Initial Response Time **
Highest	Hyperproof is experiencing a service outage or major degradation that severely impairs the usability of the product. A data integrity issue. A major, generally available feature does not work as designed and has a severe business impact. There is no workaround, or the available workaround has a severe business impact.	4 Business Hours	2 Business Hours
High	A minor performance degradation where the product is still usable but operating slower than expected.	8 Business Hours	4 Business Hours

	A major, generally available feature does not work as designed and has a high business impact. There is no workaround, or the available workaround has a high business impact.		
Medium	A major, generally available feature does not work as designed, but there is a reasonable workaround which results in a minor business impact. Use of the product for critical business operations is possible but may be more time consuming due to using a workaround. A minor, generally available feature does not work as designed and there is no workaround.	48 Business Hours	24 Business Hours
Low	Documentation issues and minor defects that have little or no business impact but are an inconvenience.	144 Business Hours	72 Business Hours

** Premium Support is an additional paid service reflected on the Order Form.

3) **Error Reporting**. Customer can report bugs and enhancements directly in the Service or report bugs and enhancements concerning the Service to their Customer Success Specialist via support@hyperproof.io.

4) **Maintenance**. Hyperproof reserves the right to limit Customer's access to the Services in order to perform maintenance or repairs, to make modifications or as a result of circumstances beyond Hyperproof's reasonable control.

5) **Services Availability**. Hyperproof agrees that the Services will be available for access and use not less than 99.5% of the time in a given year, provided that (a) that downtime due to regularly scheduled maintenance and Exclusion Events (as defined below) will not count as time during which the Services is not available, and (b) Hyperproof shall not be responsible for unavailability due to Customer's loss of Internet connectivity (the "**Uptime Commitment**"). Unavailability is the time that the Services is not available to the Customer as a function of failures in Hyperproof's or its hosting provider's hardware or software.

6) **Exclusion Events**. Hyperproof will not be responsible for any service level deficiency resulting from any of the following ("**Exclusion Events**"):

   a) A failure or interruption of any component or service for which Hyperproof is not responsible, including but not limited to, electrical power, networking equipment, computer hardware or software, or Internet and telecommunications service;
   b) Any Force Majeure event;

c) Viruses, other malicious code or denial of service attacks, unless Hyperproof fails to implement commercially reasonable threat management solutions or the service level deficiency resulted from Hyperproof's failure to property update such threat management solutions;
d) Acts or omissions of Customer or its employees, agents, third party contractors; or
e) Customer inaccessibility, where such inaccessibility either caused the problem or prevents or delays its resolution.

7) **Service Credits**. If Hyperproof fails to meet the Uptime Commitment during a month, Customer will be entitled to a credit equal to the percentage of the Monthly Fee for that month according to the schedule below ("**Service Credit**"). "**Monthly Fee**" means 1/12 of the annual subscription fee for the Licensed Product.

Uptime Percentage Service Credit

a) Equal or greater than 98.0% but less than 99.5% 10% of Monthly Fee
b) Equal or greater than 95.0% but less than 98.0% 15% of Monthly Fee
c) Less than 95.0% 20% of Monthly Fee

To be eligible for the Service Credit, Customer must notify Hyperproof within 30 days after the end of the calendar month giving rise to the Service Credit. Upon receipt of notification, Hyperproof will perform the research necessary to verify whether Customer is entitled to the Service Credit and will apply the appropriate amount to Customer's next invoice.

8) **Right to Terminate**. Customer may terminate this Agreement immediately by notice in writing to Hyperproof if:

a) Hyperproof fails to meet the Uptime Commitment more than once in any rolling period of 3 consecutive months; or
b) Hyperproof fails to meet the Uptime Commitment more than 3 times in any rolling period of 12 consecutive months. If the Agreement is terminated under this subsection (g), Hyperproof will refund to Customer any prepaid license fees for the unused portion of the Subscription Term.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into by and between the entity accepting this DPA ("**Customer**") and Hyperproof, Inc. ("**Hyperproof**"). This DPA is supplemental to the Hyperproof Main Subscription Agreement Terms and Conditions entered into between the parties which governs the provision of the Hyperproof service by Hyperproof to Customer ("**Agreement**").

1. Definitions

1.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

(a) "Applicable Data Protection Law" means all privacy and data protection laws that apply to Hyperproof's processing of Data under the Agreement (including, where applicable, the California Consumer Privacy Act of 2018 including its associated regulations and as amended (the "CCPA"), and European Data Protection Law).

(b) Controller" means the entity that determines the purposes and means of the processing of Personal Data;

(c) "Data" means Personal Data provided by Subscriber (directly or indirectly) to Hyperproof for processing under the Agreement as more particularly identified in Appendix A (Processing Particulars);

(d) "European Data Protection Law" means all EU and U.K. regulations or other legislation applicable (in whole or in part) to the processing of Personal Data under the Agreement (such as Regulation (EU) 2016/679 (the "GDPR"), the U.K. GDPR (defined below), and the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss Addendum"); the national laws of each EEA member state and the U.K. implementing any EU directive applicable (in whole or in part) to the processing of Personal Data (such as Directive 2002/58/EC); and any other national laws of each EEA member state and the U.K. applicable (in whole or in part) to the Processing of Personal Data; in each case as amended or superseded from time to time.

(e) "Model Clauses" means the standard contractual clauses attached to the European Commission's Implementing Decision of 4 June 2021 under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, on standard contractual clauses, selecting Module Two between controllers and processors in any case where Subscriber is a Controller, and Module Three between processors in any case where Subscriber is a Processor, and excluding optional clauses unless otherwise specified), and any replacement, amendment or restatement of the foregoing, as issued by the European Commission, on or after the effective date of this DPA.

(f) "Personal Data" means any information relating to an identified or identifiable natural person (a "Data Subject"), the processing of which is governed by Applicable Data Protection Law; an identifiable natural person is one who can be identified, directly or indirectly, in particular by

reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Where the CCPA applies, 'Personal Data' includes "personal information" as defined by the CCPA. Personal Data does not include anonymous or de-identified information or aggregated information derived from Personal Data. Personal Data does not include Deidentified Data (as defined in Section 2.2).

(g) "processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(h) "Processor" means an entity that processes Personal Data on behalf of the Controller. Where applicable, Processor includes "service provider" as defined by the CCPA.

(i) "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data.

(j) "Sensitive Data" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(k) "Sub-Processor" means an entity engaged by the Processor or any further sub-contractor to process Personal Data on behalf of and under the instructions of the Controller.

(l) "U.K. GDPR" means the GDPR, as it forms part of the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

2. Data Protection

2.1. *Relationship of the parties*: As between the parties and for the purposes of this DPA, Subscriber appoints Hyperproof as a Processor to process the Data on behalf of Subscriber. Where applicable, Hyperproof is a "service provider" as defined in the CCPA. Subscriber shall comply with Applicable Data Protection law, including but not limited to providing notice to Data Subjects, and obtaining and periodically refreshing the consent of Data Subjects, where required, to Subscriber's use of Hyperproof's Services and Subscriber's own processing of Data. Subscriber represents and warrants it has and will continue to have the right to transfer Data to Hyperproof for processing in accordance with the Agreement and this DPA. Hyperproof shall comply with Applicable Data Protection Law and understands and shall comply with the prohibitions on Processors set forth in the CCPA with respect to such Data, including, without limitation and to the extent applicable in each case: (i) selling or sharing any Data (as the terms "sell" and "share" are each defined within the CCPA) where the sale or sharing of such Data is restricted by the CCPA, (ii) disclosing such Data to any party outside of the direct business relationship between Hyperproof and Subscriber, or (iii) retaining, using or disclosing such Data for a commercial purpose other than performing the Services as set forth in the Agreement with Subscriber, or as otherwise expressly permitted under this DPA or the Agreement.

2.2. *Purpose limitation*: Each party acknowledges and agrees that all Data is disclosed by Subscriber hereunder only for those limited and specified purposes set forth in the Agreement and this DPA. Hyperproof shall process the Data as a Processor only as necessary to perform the Services for Subscriber under the Agreement, and strictly in accordance with the documented instructions of Subscriber (including those in this DPA and the Agreement). In no event shall Hyperproof process the Data for its own purposes or those of any third party. Hyperproof may also anonymize or deidentify Data in accordance with Applicable Data Protection Law ("Deidentified Data"), provided that Hyperproof (i) implements technical safeguards that prohibit re-identification of the Data Subject to whom the information may pertain; (ii) implements business processes that prohibit re-identification of the Deidentified Data and prevent inadvertent release of Deidentified Data; and (iii) makes no attempt to reidentify the Deidentified Data. Subscriber shall only give lawful instructions that comply with Applicable Data Protection Law and shall ensure that Hyperproof's processing of Data, when done in accordance with Subscriber's instructions, will not cause Hyperproof to violate Applicable Data Protection Law. Hyperproof shall inform Subscriber if, in its opinion, an instruction infringes Applicable Data Protection Law. In any case where confirmation of a Controller's instructions is required by Applicable Data Protection Law, the parties agree that the Agreement, together with this DPA, represents the complete and final documented instructions from the Controller of the Data to Hyperproof as of the date of this DPA for the processing of Data. Nothing in this DPA shall be read to limit any obligations of Hyperproof to assist Subscriber with Subscriber's reasonable and appropriate efforts to ensure that Hyperproof processes such Data in a manner consistent with each party's obligations under the CCPA, including (i) the obligation to immediately notify Subscriber if Hyperproof determines it can no longer meet its obligations under the CCPA with respect to such Data, and (ii) the obligation not to combine any such Data relating to a specific consumer with any other data about the same consumer in Hyperproof's possession and/or control, whether received from or on behalf of another person or persons or collected by Hyperproof from its own interaction(s) with the consumer.

2.3. *International transfers of Data*: Subscriber may select from Hyperproof's available data center locations in Subscriber's Order Form. For Hyperproof to perform Services for Subscriber pursuant to the Agreement, Subscriber transfers (directly or indirectly) Personal Data to Hyperproof in the United States, or if Subscriber elects to have Hyperproof use EU data centers, in the European Union. For Personal Data subject to European Data Protection Law, Hyperproof agrees to abide by and process the Data in compliance with the Model Clauses, which are incorporated in full by reference and form an integral part of this DPA. For the purposes of the Model Clauses, the parties agree that:

2.3.1. Hyperproof is the "data importer" and Subscriber is the "data exporter" (notwithstanding that Subscriber may itself be located outside the EEA/UK and/or a Processor acting on behalf of a third-party Controller);

2.3.2. Appendix A (Processing Particulars), and Appendix B (Specific Security Measures), of this DPA shall form Annex I and Annex II of the Model Clauses, respectively;

2.3.3. Option 2 under clause 9 of the Model Clauses will apply with respect to Sub-Processors. Annex III of the Model Clauses shall be subject to General Written Authorization, where "General Written Authorization" means that Hyperproof has Subscriber's general authorization (or the general authorization of the Controller of the Data) for the engagement of sub-processor(s) from the list set

forth in at the link specified in Section 2.7, below, which shall be amended from time to time in accordance with the terms of the Agreement, this DPA, and all Applicable Data Protection Law;

2.3.4. Audits described in clause 8.9 of the Model Clauses shall be carried out in accordance with the audit provisions detailed in Section 2.12 of this DPA;

2.3.5. The option under clause 11 of the Model Clauses shall not apply;

2.3.6. For purposes of clauses 17 and 18 of the Model Clauses, this DPA shall be governed by the laws of the Republic of Ireland . Any dispute arising from this DPA shall be resolved by the courts of the Republic of Ireland, and each party agrees to submit themselves to the jurisdiction of the same; and

2.3.7. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Model Clauses. Accordingly, if and to the extent the Model Clauses conflict with any provision of this DPA, the Model Clauses shall prevail to the extent of such conflict with respect to Personal Data processed pursuant to the Model Clauses. Subscriber warrants it will not transfer any Sensitive Data to Hyperproof which is not necessary for the use of the Hyperproof Services.

2.4. *Law enforcement requests*.

2.4.1. If Hyperproof becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "Authority") wishes to obtain access to or a copy of some or all Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Data to such Authority, Hyperproof shall: (a) promptly notify Subscriber of such Authority's data access request; (b) inform the Authority that any and all requests or demands for access to Data should be notified to or served upon Subscriber in writing; and (c) not provide the Authority with access to Data unless and until authorized by Subscriber.

2.4.2. If Hyperproof is under a legal prohibition that prevents it from complying with Section 2.4.1(a)-(c) in full, Hyperproof shall use reasonable and lawful efforts to challenge such prohibition (and Subscriber acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request). If Hyperproof makes a disclosure of Data to an Authority (whether with Subscriber's authorization or due to a mandatory legal compulsion), Hyperproof shall only disclose such Data to the extent Hyperproof is legally required to do so.

2.4.3. Section 2.4.1 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Data, Hyperproof has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Hyperproof shall notify Subscriber as soon as possible following such Authority's access and provide Subscriber with full details of the same, unless and to the extent that Hyperproof is legally prohibited from doing so;

2.4.4. Solely with respect to Data that is subject to the GDPR, and/or where Data whose disclosure is otherwise restricted by Applicable Data Protection Law, Hyperproof shall not knowingly disclose Data to an Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is

necessary in a democratic society. Hyperproof shall have in place, maintain and comply with a policy governing Personal Data access requests from Authorities which at minimum prohibits: (a) massive, disproportionate or indiscriminate disclosure of Personal Data relating to Data Subjects in the EEA and the United Kingdom; and (b) disclosure of Personal Data relating to data subjects in the EEA, and the United Kingdom to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

2.5. *Confidentiality of processing*: Hyperproof shall ensure that any person that it authorizes to process the Data (including Hyperproof's staff, agents and subcontractors) shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Data who is not under such a duty of confidentiality.

2.6. *Security*: Hyperproof shall implement appropriate technical and organizational measures to protect the Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data. Such measures shall include the security measures identified in Appendix B. For the avoidance of doubt, the parties agree that the security measures identified in Annex B are reasonable and appropriate for the processing of Data hereunder. With respect to evaluation of the appropriate level of security for the processing of the Data, each party represents and warrants that:

2.6.1. It has taken due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the Data; and

2.6.2. It has evaluated the use of encryption and/or pseudonymization for the Data and has determined that the level provided by Hyperproof is appropriate for the Data.

2.6.3. To the extent that the CCPA applies to the processing of the Data, the party has determined that the technical and organizational measures provided by Hyperproof is no less than the level of security required by the CCPA.

2.7. *Subcontracting*: Hyperproof's may subcontract the processing of Data to those third-party Sub-Processors listed at https://hyperproof.io/approvedsubprocessors. Hyperproof shall not subcontract any processing of the Data to any other third-party Sub-Processor unless Hyperproof provides at least thirty (30) days' prior notice of the addition of the Sub-Processor (including the details of the processing it performs or will perform, and the location of such processing). Notice may be provided via email to one or more Subscriber email address, as provided to Hyperproof by Subscriber. If Subscriber objects to Hyperproof's appointment of a third-party Sub-Processor on reasonable grounds relating to the protection of the Data, then either Hyperproof will not appoint the Sub-Processor, or Subscriber may elect to suspend or discontinue the affected Services by providing written notice to Hyperproof. Subscriber shall notify Hyperproof of its objection within ten (10) business days after Hyperproof's notice, and Subscriber's objection shall be sent to and explain the reasonable grounds for Subscriber's objection. If a timely objection is not made, Hyperproof will be deemed to have been authorized by Subscriber (or, if Subscriber is a Processor of the Data, by the Controller of the Data) to appoint the new Sub-Processor. Hyperproof shall impose the same data protection terms on any Sub-Processor it appoints as those provided for by this DPA and Hyperproof shall remain fully liable for any breach of Hyperproof's obligations under this DPA that is caused by an act, error or omission of its Sub-Processor.

2.8. *Cooperation and individuals' rights*: Subscriber is responsible for responding to Data Subject requests using Subscriber's own access to the relevant Data. Hyperproof shall provide all reasonable and timely assistance to enable Subscriber to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law, and (ii) any other correspondence received from a regulator or public authority in connection with the processing of the Data. In the event that any such communication is made directly to Hyperproof, Hyperproof shall promptly (and in any event, no later than within forty-eight (48) hours of receiving such communication) inform Subscriber providing full details of the same and shall not respond to the communication unless specifically required by law or authorized by Subscriber.

2.9. *Data Protection Impact Assessment*: Taking into account the nature of the processing and the information available to Hyperproof, Hyperproof shall provide Subscriber with reasonable and timely assistance with any data protection impact assessments as required by Applicable Data Protection Law and, where necessary, consultations with data protection authorities.

2.10. *Security Incidents*: Upon becoming aware of a Security Incident, Hyperproof shall inform Subscriber without undue delay and shall provide all such timely information and cooperation to enable Subscriber to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Hyperproof shall further take such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Subscriber informed of all material developments in connection with the Security Incident. Hyperproof shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) Subscriber has agreed to such notification, and/or (b) notification is required to be made by Hyperproof under Applicable Data Protection Law.

2.11. *Deletion or return of Data*: Upon termination or expiry of the Agreement, Hyperproof shall (at Subscriber's election) delete or return all Data, including copies in Hyperproof's possession or control no later than within sixty (60) days of Subscriber's election. This requirement shall not apply to the extent that Hyperproof is required by applicable laws to retain some or all of the Data, in which event Hyperproof shall isolate and protect the Data from any further processing except to the extent required by such law, shall only retain such Data for as long as it is required under applicable laws, and shall continue to ensure compliance with all Applicable Data Protection Law during such retention.

2.12. *Audit*: Hyperproof uses an external auditor to verify the adequacy of its security measures and controls for its Services. The audit is conducted annually by an independent third-party in accordance with AICPA SOC2 standards and results in the generation of a SOC2 report ("Audit Report") which is Hyperproof's confidential information. Upon written request, Hyperproof shall provide Subscriber with a copy of the most recent Audit Report subject to confidentiality obligations of the Agreement or a non-disclosure agreement covering the Audit Report. If documentation beyond the Audit Report and other information that Hyperproof provides to Subscriber is necessary to enable Subscriber to comply with its obligations with respect to the processing of Data under Applicable Data Protection Law (such as Article 28(3)(h) of GDPR where applicable), Hyperproof shall permit Subscriber to audit Hyperproof's compliance with this DPA using an independent third party and shall make available all such information, systems and staff reasonably necessary to conduct such audit. Subscriber shall not exercise its audit rights more than once per year except following a Security Incident or following an instruction by a regulator or public

authority. Subscriber shall give Hyperproof thirty (30) days prior written notice of its intention to audit, conduct its audit during normal business hours, take all reasonable measures to prevent unnecessary disruption to Hyperproof's operations, restrict findings to only data relevant to Subscriber, and provide Hyperproof with a copy of the auditor's report. Hyperproof and Subscriber shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to the audit. Subscriber shall reimburse Hyperproof for actual expenses and costs incurred to allow for and contribute to Subscriber's audit.

2.13. *Additional Terms for CCPA Data:* With respect to Data that is subject to the CCPA ("CCPA Data"), the parties acknowledge and agree as follows:

2.13.1. The terms "service providers," "sale," and "sell", as used in this section, are as defined in Section 1798.140 of the CCPA, and shall be understood as processing for purposes of this section.

2.13.2. Hyperproof will process CCPA Data for the limited and specified purposes of providing the Services under the Agreement or as otherwise permitted by the CCPA, and that, except and unless expressly permitted under this DPA, the Agreement, and the CCPA, Hyperproof shall not sell any CCPA Data, retain, use or disclose CCPA Data to any party or for any other purpose (commercial or otherwise) outside of the direct business relationship between Hyperproof and Customer. Hyperproof shall comply with all obligations of the CCPA applicable to service providers and/or contractors, including, without limitation:

(a) notifying Customer if Hyperproof determines it can no longer meet its obligations under the CCPA;

(b) not combining the CCPA Data relating to a specific consumer with any other data about the same consumer in Hyperproof's possession and/or control, whether received from or on behalf of another person or persons or collected by Hyperproof from its own interaction(s) with the consumer; and

(c) ensuring that each and all persons authorized by Hyperproof to access the CCPA Data (which may include, without limitation, Hyperproof's employees, independent contractors, Sub-Processors, agents, and other personnel) complies with all of the foregoing obligations.

(d) to the extent required by the CCPA, assisting Customer in taking reasonable and appropriate steps (i) to stop and remediate unauthorized use of the Data, and (ii) to ensure that Hyperproof processes the Data in a manner consistent with Customer's obligations under the CCPA.

2.14. Additional Terms for U.S. Laws: With respect to Data that is subject to U.S. specific data protection laws, Customer agrees that it shall adhere to Customer's instructions in the processing of such Personal Data to the extent required to comply with such laws, and shall assist Customer in meeting its obligations under applicable U.S. specific data protection laws on the terms described in this DPA.

3. Miscellaneous

3.1 The obligations placed upon the Hyperproof under this DPA shall survive so long as Hyperproof and/or its sub-Processors process Personal Data on behalf of Customer.

3.2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

3.3. It is not the intention of either party, nor shall it be the effect of this DPA, to contradict or restrict any provision of the Model Clauses and/or any Applicable Data Protection Law. To the extent that any provision of the Model Clauses conflicts with this DPA, the Model Clauses shall prevail to the extent of such conflict with respect to Personal Data which is subject to the Model Clauses. In no event shall this DPA restrict or limit the rights of any Data Subject or of any Authority. If there is a change in law requiring any change to this DPA to enable either party to continue to comply with Applicable Data Protection Law, the parties will negotiate in good faith to amend this DPA to the extent reasonably necessary to comply with Applicable Data Protection Law.

3.4. If any provision of this DPA is deemed invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended to ensure its validity and enforceability while preserving the parties' intentions as closely as possible; or (ii) if that is not possible, then construed in a man-ner as if the invalid or unenforceable part had never been included herein.

3.5. The term of this DPA will terminate automatically without requiring any further action by either party upon the later of (i) the termination of the Agreement, or (ii) when all Personal Data is removed from Hyperproof's systems and records, and/or is otherwise rendered unavailable to Hyperproof for further Processing.

ANNEX A: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex A includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Customer Data

The subject matter and duration of the processing of the Customer Data are set out in the Hyperproof Main Subscription Agreement and this Addendum.

The nature and purpose of the processing of Customer Data

The nature and purpose of the processing of Customer Data are set out in the Hyperproof Main Subscription Agreement and this Addendum.

The types of Customer Data to be processed

Customer may submit Personal Data, the extent of which is determined and controlled by Customer (including Customer's Users and Customers) in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

- Identification and contact data (name, title, address, phone number, email address);

- Employment data (employer, job title, academic and professional qualifications, geographic location, area of responsibility, affiliated organization, area of responsibility and industry);
- Purchase and usage history data;
- IT related data (IP addresses of visitors to data exporter's customer's websites, online navigation data, browser type, language preferences, pixel data, cookies data, web beacon data);
- IT information (computer ID, user ID and password, domain name, IP address, log files, software and hardware inventory, software usage pattern tracking information (ie cookies and information recorded for operation and training purposes); and,
- If the parties mutually agree on expanded use case, financial information (account details, payment information.

The categories of Data Subject to whom the Customer Data relates

Customer may submit Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- Employees, agents, advisors, freelancers of Customer (who are natural persons); and
- Customer's Users, Partners, Hyperproof's, and Customers and the users and employees of those entities.

The obligations and rights of Customer

The obligations and rights of Customer are set out in Hyperproof Main Subscription Agreement and this Addendum.

ANNEX B

SPECIFIC SECURITY MEASURES

1. Description of the technical and organizational security measures implemented by the Hyperproof:

Hosting and Physical Security

Hyperproof application servers are hosted on Microsoft Azure. As such, Hyperproof inherits the control environment which demonstrates numerous US, worldwide, and government certifications including SOC 1, 2 and 3, ISO 27001, FedRAMP, HIPAA, HITRUST, PCI, GDPR and more. Web servers and databases run on servers in secure data centers. Physical access is restricted to authorized personnel. Premises are monitored and access is logged. Additional information regarding Azure compliance can be found at https://docs.microsoft.com/en-us/azure/compliance.

Hyperproof utilizes Twilio SendGrid for email notification services. SendGrid has SOC 2 Type 2 certification. Additional information regarding SendGrid can be found at https://sendgrid.com/policies/security.

Hyperproof utilizes Elastic.co for logging and monitoring but does not store customer data or PII in the Elastic service. Elastic is also hosted on Microsoft Azure. Elastic has a SOC2 Type 2 and HIPAA certifications. Additional information regarding Elastic security and certifications can be found at https://www.elastic.co/cloud/security.

Isolation of Services

Hyperproof servers run in Linux containers in the Azure Kubernetes Service which are isolated from one another and from the underlying hardware layer. Each service runs in its own container and does not have access to the process or filesystem storage of any other service.

Network Security

Hyperproof services are accessible only over HTTPS using TLS 1.2 or above. Traffic over HTTPS is encrypted and is protected from interception by unauthorized third parties. Hyperproof uses only strong encryption algorithms with a key length of at least 256 bits.

All network access, both within the data center and between the data center and outside services, are restricted by firewall and routing rules. Network access is logged, and logs are retained for a minimum of 30 days.

Hyperproof servers are only accessible through HTTPS using TLS 1.2 or above and deny access to other ports, except that remote management access (protected by TLS 1.2 or above and two factor login authentication) is enabled for administration. Administrative access is granted only to select employees of Hyperproof, based on role and business need.

All employees with administrative access must pass a criminal background check at every year.

Authentication

Clients login to Hyperproof using a password which is known only to them and done only over secure (HTTPS) connections. Clients are required to have strong passwords when not using SSO. Passwords are not stored unencrypted; instead, as is standard practice, only a secure hash of the password is stored in the Azure B2C directory utilized by the Hyperproof service. The Hyperproof service and Hyperproof employees never have access to client passwords or their hashes.

When clients enable end users to connect to Hyperproof using user-supplied credentials (Single Sign On), this is done using security tokens, OAuth, or SAML 2.0, and in those cases, no credentials need to be stored in the Hyperproof system.

Development Process

Hyperproof developers have been trained in secure coding practices. Hyperproof application architecture includes mitigation measures for common security flaws such as the OWASP Top 10 and entries the CVE database. The Hyperproof application uses industry standard, high-strength algorithms including AES for all data encryption. Hyperproof undergoes penetration testing at least once per year.

Employee Screening and Policies

As a condition of employment all Hyperproof employees with access to code, hosted services, or customer data undergo criminal background checks background checks. All Hyperproof employees take mandatory security training and agree to company policies including security and acceptable use policies.

Security Issues

At Hyperproof, we consider the security of our systems a top priority. We have implemented a responsible disclosure policy to ensure that problems are addressed quickly and safely.

ANNEX C

COMPETENT SUPERVISORY AUTHORITY

For the purposes of any Personal Data subject to the GDPR and/or the GDPR as implemented in the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018, where such personal data processed in accordance with the Model Clauses, the competent supervisory authority shall be as follows:

(i) where Subscriber is established in an EU member state, the supervisory authority with responsibility for ensuring Subscriber's compliance with the GDPR shall act as competent supervisory authority;
(j) where Subscriber is not established in an EU member state, but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU member state in which Subscriber's representative is established shall act as competent supervisory authority; or
(k) where Subscriber is not established in an EU member state but falls within the extra-territorial scope of the GDPR without however having to appoint a representative, the supervisory authority of the EU member state in which the Data Subjects are predominantly located shall act as competent supervisory authority.

In relation to Personal Data that is subject to the U.K. GDPR, the competent supervisory authority is the United Kingdom Information Commissioner's Office, subject to the additional terms set forth in the International Data Transfer Addendum to the EU Model Clauses attached hereto as "Appendix D".

In relation to Personal Data that is subject to the data privacy laws of Switzerland, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

ANNEX D

U.K INTERNATIONAL DATA TRANSFER ADDENDUM

This U.K. INTERNATIONAL DATA TRANSFER ADDENDUM ("IDTA") forms a part of the Data Processing Addendum ("DPA") entered into by and between Hyperproof, Inc. ("Hyperproof") and the party identified as the Subscriber in the DPA ("Subscriber"). Unless otherwise specified, all capitalized terms used in this IDTA have the meanings provided in the DPA.

1. *Scope of IDTA*. The obligations set forth in this IDTA apply solely to Personal Data subject to the U.K. GDPR that is processed under the DPA ("U.K. Personal Data").
2. *Incorporation of the U.K. Addendum*. The parties agree that the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the U.K. Information Commissioner's Office under s.119A (1) of the U.K. Data Protection Act 2018 ("U.K. Addendum") is incorporated by reference into and forms a part of this IDTA as if fully set forth herein. Each party agrees that execution of the DPA (to which this IDTA is attached as an appendix and incorporated by reference) shall have the same effect as if the parties had simultaneously executed a copy of the U.K. Addendum.
3. *Interpretation of the Model Clauses*. For purposes of Processing U.K. Personal Data, any references in the DPA to the Model Clauses shall be read to incorporate the mandatory amendments to the Model Clauses set forth in the U.K. Addendum.
4. *Addendum Terms*. Tables 1 through 4 of the U.K. Addendum shall be completed as follows:
    (a) In Table 1 of the U.K. Addendum, the "Start Date" shall be the Effective Date of the DPA, and the details and contact information for the "data exporter" and the "data importer" shall be as specified in Appendix I of the DPA.
    (b) In Table 2 of the U.K. Addendum:
        I. The version of the Model Clauses incorporated by reference into the DPA shall be the version applicable to this IDTA.
        II. Those provisions of the Model Clauses applicable under Module Two shall apply to this IDTA.
        III. The optional clauses and provisions of the Model Clauses applicable to this IDTA shall be those clauses and provisions specified in Section 2.3 of the DPA.
    (c) In Table 3 of the U.K. Addendum, the information required in Annexes I (both 1A and 1B), II, and III shall be as provided in Appendices A, B, and C of the DPA, respectively.
    (d) In Table 4 of the U.K. Addendum, if the ICO issues any revisions to the U.K. Addendum after the Effective Date ("ICO Revision"), Subscriber and Hyperproof shall each have the right to terminate this IDTA in accordance with the U.K. Addendum, the DPA, and the Agreement. Upon such termination of this IDTA:
        I. Hyperproof shall cease its Processing of the U.K. Personal Data; and
        II. Each party shall follow the processes described in Section 2.11 of the DPA with respect to the U.K. Personal Data.

Notwithstanding the foregoing, termination of this IDTA in the event of an ICO Revision shall not terminate the DPA, the Agreement, and/or the obligations of either party arising thereunder with respect to Personal Data other than U.K. Personal Data, except and unless expressly agreed by and between the parties.

5. *No Amendments*. The terms of the U.K. Addendum have not been amended in any way except as expressly stated herein