



SOFTWARE AS A SERVICE LICENSE AGREEMENT

LICENSOR PROVIDES THE SERVICE (AS DEFINED BELOW) SOLELY ON THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT AND ON THE CONDITION THAT LICENSEE ACCEPTS AND COMPLIES WITH THEM.

BY PLACING A PURCHASE ORDER FOR THE SERVICE OR BY ACCESSING OR USING THE SERVICE OR BY CLICKING THE "ACCEPT" BUTTON ON THE LOG-IN SCREEN, YOU AGREE TO BE BOUND BY THESE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS USERS (AS DEFINED BELOW) TO THESE TERMS AND CONDITIONS, IN WHICH CASE "CUSTOMER" SHALL MEAN SUCH ENTITY AND ITS USERS OR PERSONS USING SUCH SERVICES ON ITS BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT AGREE WITH THESE TERMS, YOU SHALL NOT ACCESS OR USE THE SERVICE.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR YOUR OR LICENSEE'S ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, NO LICENSE IS GRANTED (WHETHER EXPRESSLY, BY IMPLICATION OR OTHERWISE) UNDER THIS AGREEMENT, AND THIS AGREEMENT EXPRESSLY EXCLUDES ANY RIGHT CONCERNING ANY SOFTWARE THAT LICENSEE DID NOT ACQUIRE LAWFULLY OR THAT IS NOT A LEGITIMATE, AUTHORIZED COPY OF LICENSOR'S SOFTWARE.

This Software as a Service License Agreement (the "**SaaS Agreement**") and, together with all addenda and documents incorporated herein by reference, the "**Agreement**") governs Customer's license to access and use the Revvity Health Sciences, Inc. (together with its affiliates and subsidiaries, "**Licensor**" or "**Revvity**") software as a service offering identified on the applicable quote ("**Quote**"), together with any published user guide and/or technical manual for the software as a service offering (the "**Documentation**") and, together, the "**Service**"), in accordance with the following terms and conditions and any applicable specific terms and conditions attached hereto as an Annex.

1. LICENSE GRANT. Subject to Customer's payment obligations and the terms and conditions of this Agreement, Revvity hereby grants to Customer a limited, revocable, non-transferable, and non-exclusive license to access and use the Service for the duration of Customer's purchased subscription term for Customer's internal business purposes only. This license is for use of the Service by Customer and Customer's employees, agents, representatives, contractors, or consultants who are authorized by Customer to access and use the Service in accordance with any terms and restrictions for such use as set forth in the Quote ("**User(s)**"). Customer shall ensure and is responsible for its Users' compliance with the terms and conditions of this Agreement, and any act or omission by a User that would constitute a breach of this Agreement if taken by Customer shall be deemed a breach of this Agreement by Customer.

2. ACCESS AND USE RESTRICTIONS. Neither Customer nor its Users will take any action or inaction that actually or attempts to: (a) interfere with, disrupt, diminish the quality of, or impair the performance or functionality of the Service; (b) circumvent, disable, or interfere with (i) security-related features of the Service, (ii) features that prevent or restrict use, access to, or copying of any data, or (iii) features that enforce limitations on use of the Service or data; (c) monitor or sample the performance or security response of the Service or stress tests APIs; or (d) violates Revvity's Acceptable Use Policy, attached hereto and incorporated herein ("**AUP**"). Customer agrees not to, and shall ensure its Users do not, directly or indirectly, in whole or in part: (a) copy, distribute, modify, translate, create derivative works of, reverse engineer, decrypt, decompile, disassemble, or in any way attempt to derive the source code of any software related to the Service or underlying ideas, techniques, or algorithms, including the review of data structures or similar materials produced by the Service, (b) sub-license, lease, rent, loan, sell, distribute, transfer, or commercially share (including time-share or electronically transmitting over a network to a third party) or otherwise permit use of the Service in connection with a service bureau or other configuration whereby any third party may use the Service; (c) use versions of third party products embedded in the Service, if any, for any use other than the intended use of the Service; (d) combine any software related to the Service with other software that, under the license applicable to such software, requires as a condition of use, modification, or distribution that such combined software is required to be: (i) disclosed or distributed in source code form, (ii) freely licensed for the purpose of making derivative works, or (iii) redistributable at no charge (including but not limited to any software that is distributed as free software, open source software or similar licensing or distribution models); (e) use the Service in any ultra-hazardous activity; or (f) release the results of benchmark testing using the Service, except to the extent such restriction is prohibited by applicable law. Customer and its Users will comply with all local, state, federal, national, international or supranational laws, statutes, ordinances, or regulations that apply to its use of the Service, the Customer Data (as defined below), and any content posted within the Service by Revvity or on its behalf or to which



Customer may be exposed due to Customer's use of the Service ("**Content**"). Neither Customer nor its Users shall use the Service in any manner or for any purpose other than as expressly permitted by this Agreement.

3. SERVICE ACCESS. (a) Customer will provide its own Internet access with sufficient connectivity and all communications equipment, computer systems, software, and other materials ("**Computer Systems**") necessary for it and its Users to access and use the Service. Customer is solely responsible for the security of its own Computer Systems and the security of its access to and connection with the Service. (b) Each User will have a unique user ID and password to access the Service, and Customer will ensure that its Users will use only their respective assigned user IDs and passwords and not those of another User. Customer is responsible for maintaining the security and confidentiality of all usernames, passwords, and access keys for the use of the Service. Customer shall not disclose or make available passwords other than to its Users, shall use best efforts to prevent unauthorized access to or use of the Service, and will promptly notify Revvity of any unauthorized use, loss or theft of any username, password, or access key, or any other known or suspected breach of security. In the event Customer makes such passwords available to any third-party, Customer shall be solely liable for all actions taken by such third party.

4. CUSTOMER DATA. All data entered, uploaded or otherwise submitted to the Service by Customer, its Users or otherwise on Customer's behalf ("**Customer Data**") will remain the sole property of Customer and is entered, uploaded or otherwise submitted at Customer's sole risk. Revvity is not responsible for the accuracy, completeness or integrity of Customer Data. Revvity does not warrant the accuracy or completeness of data in reports generated using Customer Data, and Customer is solely responsible for data validation in any reports designed or generated by Customer using the Service. **REVVITY EXPRESSLY DISCLAIMS RESPONSIBILITY AND LIABILITY FOR THE RESULTS OBTAINED THROUGH REPORTS DESIGNED OR GENERATED BY CUSTOMER USING THE SERVICE'S REPORTING FUNCTIONALITIES.**

Except as set forth in Section 10 of this Agreement, any requests for exports of Customer Data in Revvity's standard format, or requests for exports of Customer Data in any format other than Revvity's standard format, may be performed by Revvity at Customer's sole cost and expense.

For the sole purpose of enabling Revvity to provide Customer and its Users with the Service and to perform any maintenance, support, or Professional Services (as defined below) purchased by Customer hereunder, Customer grants to Revvity the right to use, process, transmit, host, copy, and display any Customer Data in accordance with this Agreement, for the duration of the subscription term and as necessary during any additional post-termination period, if and to the extent Revvity agrees to assist Customer in the wind-down of its use of the Service.

5. SECURITY AND PRIVACY ADDENDUM. Revvity shall take those actions to protect the Services and Customer Data as set forth in the Security and Privacy Addendum, attached hereto and incorporated herein ("**Security Addendum**"). Customer acknowledges that Customer is solely responsible for taking any additional measures it deems advisable or appropriate to secure and back up its systems to prevent any loss of files or Customer Data during Customer's subscription term. Customer is additionally responsible for any security vulnerabilities and the consequences of such vulnerabilities arising from Customer Data, including any viruses, Trojan horses, worms or other programming routines contained in Customer Data that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data.

6. OWNERSHIP; INTELLECTUAL PROPERTY RIGHTS. The Service is copyrighted and contains proprietary information protected by law. Ownership of and title to the Service are and shall remain with Revvity or its licensors at all times, and Customer acknowledges that Revvity or its licensors own all rights to: (i) the Service and Service website, (ii) all software, databases, and tangible and intangible materials embodied in or relating to the Service, including without limitation all raw, gross or compiled statistical information, aggregate anonymous statistical data regarding use and functioning of the Service, and other data relating to the Services generally that is obtained, assembled or developed by Revvity in the course of providing its services (but excluding Customer Data), and (iii) all software modifications, Improvements (as defined below), and derivative works; and all copyright, patent, trademark, trade secret, and other intellectual property or other rights in and to each of the foregoing (collectively, the "**Revvity Intellectual Property**"). Nothing contained in this Agreement will be construed to convey any title or ownership right in any Revvity Intellectual Property to Customer, or any right to use any of the Revvity Intellectual Property other than as expressly set forth in this Agreement. Revvity may modify, amend, or change its applications, products, services, and the Service at its sole discretion and without notice. Revvity hereby reserves all rights not expressly granted to Customer hereunder.



The Service may operate or interface with software or other technology which is not proprietary to Revvity and is licensed to Revvity by third parties ("**Third Party Licensors**"), but for which Revvity has the necessary rights to license to Customer ("**Third Party Software**"). Customer agrees that (i) Customer and its Users will use such Third Party Software in accordance with this Agreement, (ii) no Third Party Licensor makes any warranties or representations of any kind, either express or implied, to Customer concerning such Third Party Software or the Service itself, (iii) no Third Party Licensor will have any obligation or liability to Customer as a result of this Agreement or Customer's use of such Third Party Software, and (iv) such Third Party Software may be licensed under license terms which grant Customer additional rights or contain additional restrictions in relation to such materials beyond those set forth in this Agreement, and such additional license rights and restrictions are described or linked to within the applicable documentation, the relevant webpage, or within the Service itself. Neither Customer nor its Users shall remove or modify any of Revvity's or its licensors' marks or proprietary notices contained in or on the Service or in any documentation or materials made available to Customer related to the Service.

Any custom configurations, integrations or modifications developed by Revvity for the Customer shall be deemed works made for hire owned by Revvity, and Customer receives only the license rights expressly granted here.

7. PROFESSIONAL SERVICES. Subject to the terms of a mutually agreed and executed statement of work or a Revvity quote for or including professional services (each, a "**SOW**"), Revvity may from time to time provide to Customer professional services, including the delivery of any applicable deliverables ("**Deliverables**") as may be described in such SOW or quote ("**Professional Services**"). Unless the parties have mutually executed a separate Master Services Agreement applicable to such Professional Services, each SOW shall be subject to the terms and conditions of this Agreement and shall be incorporated herein by reference. Customer is responsible for providing accurate and complete information as required or requested by Revvity for the provision of Professional Services, and Revvity shall not be liable or responsible for any delays or technical difficulties arising from Customer's failure to provide such accurate and complete information. Revvity may include its pre-existing Software, Third Party Software, or other materials in the Deliverables. All Deliverables, including improvements, derivatives and modifications to such thereto, shall remain the property of Revvity, and Customer will receive a fully paid, royalty-free license to use such Deliverables in accordance with the terms of this Agreement.

8. MAINTENANCE AND SUPPORT. Revvity will provide to Customer standard electronic technical support for the Service as set forth in the Service Level Addendum, attached hereto and incorporated herein ("**SLA**"). Customer is required to accept all patches, bug fixes, updates, maintenance and service packs (collectively, "**Patches**") necessary for the proper function and security of the Service as such Patches are generally released by Revvity.

9. FEES AND PAYMENT. The Service fees are payable in advance according to the subscription plan Customer has selected and the payment schedule set forth on the Quote and payable in U.S. Dollars. Except as set forth in Section 10 below, payment obligations are non-cancellable and non-refundable, and quantities purchased cannot be decreased during the subscription term set forth on the Quote. Customer is responsible for all bank transfer fees or any withholding taxes required by applicable law. Customer agrees that Customer's subscription purchase and obligation to pay is not contingent on the delivery of, or any oral or written representations made by Revvity regarding, any future functionality or features or on performance of any other service offerings or delivery of other programs or products by Revvity. Customer agrees to promptly notify Revvity if its usage of the Service exceeds the contracted volume or data storage limits applicable to the Service and will promptly pay all fees associated with such excess usage. Subscriptions may be added or increased during a subscription term at the same pricing as the underlying subscription pricing for the purchased Service, and the price payable for such added subscription shall be pro-rated (if applicable) for the term remaining on the underlying subscription. Any added or increased subscriptions will terminate on the same date as the underlying subscriptions. Payment for fees and expenses is subject to a late charge of One and One-half Percent (1½%) per month or the maximum permitted under applicable law if unpaid for thirty (30) days or more from invoice date. Revvity reserves the right to change the pricing for the Service for any renewal or future subscription term. All fees are exclusive of all taxes, levies, or duties imposed by taxing authorities, and Customer shall be responsible for the payment of all such taxes, levies, and duties, excluding taxes based upon the net income of Revvity.

10. TERM; TERMINATION; SUSPENSION. This Agreement shall become effective on the date Customer places its first purchase order for the Service and will expire at the end of the last subscription term to expire, unless extended by the parties for the duration of any renewal subscription terms purchased by Customer or terminated earlier as set forth herein.



Either party may earlier terminate the Service (i) for its convenience with ninety (90) days prior written notice or (ii) with written notice to the other party if such party materially breaches this Agreement, and such breach remains uncured thirty (30) days following receipt of written notice specifying such breach. Revvity may immediately terminate the Service without liability hereunder if Customer or its Users breach Section 2 or Section 11 of this Agreement. Revvity may additionally terminate this Agreement with reasonable written notice if Revvity ceases to provide the Service generally.

Upon expiration or termination of this Agreement, Customer's rights to access and use the Service shall automatically and immediately terminate, and Customer shall immediately (i) cease use of the Service; (ii) delete all copies of documentation made available to Customer by Revvity; and (iii) at Customers' expense, return to Revvity all Confidential Information and data of Revvity (including all copies thereof) then in Customer's possession, custody or control, and certify in writing as to such action within thirty (30) days of termination. No later than thirty (30) days following termination or expiration of the affected Service, Customer may request a one-time export of Customer Data from the Service in Revvity's standard format at no charge to Customer. If Revvity does not receive such request within thirty (30) days of expiration or termination of the affected Service, Revvity may destroy, delete or otherwise render inaccessible all Customer Data in its possession, custody or control without liability hereunder. Customer may receive a refund of any fees pre-paid by Customer for the period of the subscription term remaining following the effective date of termination for the affected Service if: (i) Revvity terminates this Agreement or the Service for its convenience; (ii) Revvity ceases to provide the Service generally; or (iii) Customer terminates this Agreement or Service due to Revvity's material uncured breach. Any other suspension or termination of the Service by Customer or Revvity shall not relieve or excuse Customer from its obligation to make payment(s) under this Agreement.

Revvity may suspend Customer's access to or use of the Service without liability hereunder if Customer or any User violates any provision of this Agreement, including failure to pay fees due hereunder, or, in Revvity's reasonable judgment, if the Service or any component thereof is about to suffer significant threat to security or functionality. If practicable and permitted under applicable law, Revvity will provide advance notice to Customer of any such suspension. Revvity will use reasonable efforts to re-establish the affected Service promptly after Revvity determines that the situation giving rise to the suspension has been cured. Revvity may terminate the Service if any of the foregoing causes of suspension are not cured within thirty (30) days after Revvity's initial notice thereof. If Revvity suspends, terminates, or prevents access to Customer's account, Customer must not attempt to re-register or submit content or Customer Data (e.g., using someone else's registration), without Revvity's prior permission. The period of any suspension will be determined at Revvity's reasonable discretion based on the applicable facts and circumstances.

Provisions that survive termination or expiration of this Agreement are those relating to limitation of liability, indemnification, confidentiality, ownership, payment, and others which by their nature are intended to survive. Upon expiration or termination, Revvity will be entitled to discontinue prospective hosting of Customer Data.

11. PRIVACY. If the Customer intends to use the Service to process personal or health data subject to protection under the laws of any country or the European Union, Customer agrees that it shall (i) inform Revvity promptly and, if required under applicable law, enter into any additional agreement required under such law (the "DPA"); and (ii) not provide to Revvity or transmit or enter into the Service any personal or health information of any person in violation of any applicable data privacy regulations. For Customers in the United States, if Customer is a Covered Entity or Business Associated under the Health Insurance Portability and Accountability Act of 1996, as amended and its implementing regulations including the HITECH Act of 2009 and the HIPAA Omnibus Rule of 2013, collectively "HIPAA", Customer shall notify Revvity prior to submitting any Protected Health Information or Electronic Protected Health Information through the Service and the Parties will negotiate and execute a Business Associate Agreement ("BAA") in good faith prior to any such processing. Any submission of PHI or ePHI in violation of this Section shall constitute a material breach of this Agreement.

12. FEEDBACK. Revvity may use, disclose, and exploit any and all suggestions, ideas, recommendations, enhancement requests, corrections, improvements, modifications, error identifications, or other information provided by Customer to Revvity related to the Service or any other products or services, and any data or information relating to Customer's use of the Service (collectively, "Feedback"), including to improve the Service and to develop, market, offer, sell or provide other products or services, without restriction and without accounting to Customer. Revvity shall be the sole and exclusive owner of all improvements, updates, modifications, or enhancements made to the Service, whether or not conceived or made as a result of Customer's Feedback hereunder, and of all intellectual property rights therein (collectively, the "Improvements"), and no right, title or interest in or to the Improvements is expressly or impliedly granted to Customer



hereunder. Customer acknowledges and agrees that Revvity is free to incorporate into any commercial products and services any Feedback suggested by Customer or Improvements, and that Customer has no right to object thereto or to receive any form of compensation derived therefrom. To the extent permitted by applicable law, Customer waives and agrees not to assert any moral rights in any Feedback.

13. CONFIDENTIALITY. “Confidential Information” means, in the case of Revvity, (i) all components of the Service; (ii) Revvity Intellectual Property and Improvements; (iii) all other proprietary documentation and information relating to or exchanged during the subscription term, including the Feedback; and (iv) the terms of this Agreement; in the case of Customer, (v) all proprietary Customer-specific information and (vi) Customer Data; and, in each case and as applicable, (vii) any other information or material disclosed or made available by either Revvity or Customer that should reasonably be understood to be confidential. Confidential Information does not include information (i) already known to the receiving party before the date of disclosure; (ii) generally available to the public; (iii) shown through documentation to have been developed by the receiving party independent of the received Confidential Information; or (iv) received without obligations of confidentiality from a third party legally entitled to disclose it. Except as permitted by this Agreement, neither Revvity nor Customer will disclose to any entity or person (except its employees, representatives, agents, or contractors who have a need to know the Confidential Information and who are subject to confidentiality obligations no less restrictive than those set forth herein) or use any Confidential Information it receives from the other party hereunder. Revvity and Customer will each exercise the same degree of diligence as it exercises in protecting its own confidential information, but no less than reasonable efforts, to safeguard the Confidential Information and to prevent its unauthorized use or disclosure. Customer’s confidentiality obligations include an obligation not to use Revvity’s Confidential Information to develop, assist in developing, or procure development of any product or service competitive with the Service. This section shall survive the expiration or termination of the Agreement.

14. WARRANTY; WARRANTY DISCLAIMER. Revvity warrants that: (i) the software as a service offering will substantially conform to the material features and functionality set forth in the Documentation, and (ii) it shall perform all Professional Services in a professional, workmanlike manner in accordance with generally recognized industry standards. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 14, THE SERVICE AND PROFESSIONAL SERVICES ARE PROVIDED “AS IS,” “AS AVAILABLE,” AND WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. REVVITY DOES NOT WARRANT THAT THE SERVICE (A) WILL OPERATE ERROR- FREE OR UNINTERRUPTED (INCLUDING WITHOUT LIMITATION DUE TO NETWORK OUTAGES OR THIRD PARTY FAILURES AND/OR DELAYS) OR THAT REVVITY WILL CORRECT ALL SERVICE ERRORS; (B) WILL MEET CUSTOMER’S REQUIREMENTS, SPECIFICATIONS OR EXPECTATIONS, OR (C) WILL ACHIEVE ANY INTENDED RESULT; AND CUSTOMER AGREES THAT IT WILL MAKE NO CLAIM AGAINST REVVITY BASED ON USE OF THE SERVICE.

CUSTOMER ACKNOWLEDGES THAT REVVITY DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES FOR WHICH REVVITY IS NOT RESPONSIBLE OR LIABLE. REVVITY IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION, OR SECURITY OF THE SERVICE THAT ARISE FROM, AND DOES NOT MAKE ANY WARRANTIES REGARDING, CUSTOMER’S DATA OR THIRD-PARTY CONTENT AND HEREBY DISCLAIMS ALL LIABILITIES ARISING FROM OR RELATED TO THIRD PARTY CONTENT OR SERVICES (INCLUDING THIRD PARTY HOSTING PROVIDERS). SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN IMPLIED WARRANTIES AND THEREFORE REVVITY’S LIABILITY IS LIMITED TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

Any warranty claim must be submitted within sixty (60) days of the alleged non-conformance.

The following warranty terms shall additionally apply to the Revvity’s Transcribe AI Service:

NO WARRANTY. Revvity does not warrant the accuracy or completeness of the customer data, reports, outputs, or interpretation submitted to the Service. Customer assumes sole responsibility for data validation and data accuracy in any reports designed or generated by Customer using the Service. REVVITY EXPRESSLY DISCLAIMS RESPONSIBILITY AND LIABILITY FOR THE RESULTS GENERATED BY CUSTOMER USING THE SERVICE’S



FUNCTIONALITIES.

CUSTOMER DATA TRANSCRIBED BY THE SERVICE IS AS IS, WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED. REVVITY SHALL HAVE NO LIABILITY FOR, NOR DOES REVVITY GUARANTEE, THE ACCURACY, RELIABILITY, FUNCTIONALITY, ERRORS, OR ISSUES ARISING FROM THE USE OF THE SERVICE. IT IS THE CUSTOMER'S RESPONSIBILITY FOR THE FUNCTIONALITY, ACCURACY, OR IMPACT OF THE SERVICE ON CUSTOMER'S BUSINESS OR OPERATIONS. IT IS RECOMMENDED TO CUSTOMER THAT ANY REPORTS, RESULTS, OUTPUTS OR OTHERWISE GENERATED BY THE SERVICE BE VALIDATED BY A HUMAN.

15. REMEDIES; LIMITATION OF LIABILITY. Revvity will not be responsible or liable for any Service problems or issues arising from (i) use of the Service by Customer or any User in breach of this Agreement; (ii) modification, alteration, or configuration of the Service by or for Customer that has not been authorized in writing by Revvity; (iii) hardware, software, technology, intellectual property, communications facilities, or equipment which has not been provided by Revvity; (iv) any act or omission of Customer or any User that prevents, delays, disturbs, or interferes with Revvity's performance of its obligations hereunder; or (v) performance or security issues encountered with the Service that result from Customer's failure to accept the application of Patches that are necessary for the proper function and security of the Service.

If the Services or Professional Services fail to meet the express warranties set forth in this Section 15, Revvity will, in Revvity's sole discretion and as Customer's sole and exclusive remedy, either (i) correct the non-conformities in the Service in accordance with the SLA, or re-perform the affected Professional Services; or (ii) terminate the affected Service or SOW and provide to Customer a refund for the remaining duration of the purchased subscription term or for the affected portion of the Professional Services, as applicable. For clarity, Customer's sole and exclusive remedies for breach of the SLA are as set forth in the SLA.

EXCEPT IN CONNECTION WITH (A) CUSTOMER'S BREACH OF SECTION 2, (B) A PARTY'S INDEMNIFICATION OBLIGATIONS HEREUNDER, OR (C) A PARTY'S BREACH OF SECTION 13, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF REVENUE, LOSS OF PROFITS (EXCLUDING FEES PAYABLE OR DUE UNDER THIS AGREEMENT), DATA LOSS, BREACH OF DATA OR SYSTEM SECURITY, OR DATA USE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AVAILABLE REMEDIES ARE FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

IN NO EVENT WILL REVVITY BE LIABLE FOR ANY DAMAGES, WHETHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL, OR FOR ANY LOSS OF PROFITS, REVENUE, DATA OR DATA USE, ARISING FROM THE USE OF THE SERVICE OR THIRD-PARTY SOFTWARE. REVVITY'S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT, OR OTHERWISE, SHALL BE LIMITED TO THE TOTAL AMOUNTS ACTUALLY PAID BY CUSTOMER OR PAYABLE TO REVVITY FOR THE SERVICE GIVING RISE TO THE LIABILITY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE OCCURRENCE OF THE CAUSE OF ACTION.

IN NO EVENT WILL REVVITY'S LIABILITY FOR BREACHES OF SECTION 13 EXCEED TWO TIMES THE TOTAL AMOUNTS ACTUALLY PAID BY CUSTOMER OR PAYABLE TO REVVITY FOR THE SERVICE GIVING RISE TO THE LIABILITY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE OCCURRENCE OF THE CAUSE OF ACTION.

16. INDEMNIFICATION.

(a) Indemnification of Customer by Revvity. Revvity shall indemnify and defend Customer, its affiliates, and their respective officers, agents, employees, subsidiaries, assigns, and successors in interest (collectively, "**Customer Indemnitees**") against, and hold Customer Indemnitees harmless from, all liabilities, losses, and damages, including reasonable attorneys' fees and costs (collectively, "**Losses**") awarded against Customer Indemnitees in a final judgment resulting from any third party claim, suit, or proceeding to the extent alleging that the Service or use of the Service, as permitted hereunder and in accordance with the Documentation, infringes or misappropriates the intellectual property rights of such third party, unless and except to the extent that such infringement is caused by (i) the Service or Documentation being modified by a Customer Indemnitee or on its behalf or used by a Customer indemnitee or a third party on its behalf outside the scope of use identified in Revvity's Documentation; (ii) Revvity's compliance with Customer indemnitee's instructions or requests or Revvity's use of trademarks, Customer Data, content or other materials supplied by any Customer Indemnitee; (iii) the combination of the Service with any products or services not provided by Revvity; or



(iv) any Customer Indemnitee's actions or inactions if the Service and/or Documentation as delivered to Customer would not otherwise infringe such third party's intellectual property rights. In the event of a claim under this Section 16(a), Revvity has the right to (i) obtain a license to allow for Customer's continued use; (ii) modify the Service or Documentation so that it no longer infringes such third party's intellectual property rights; or (iii) if these alternatives are not commercially reasonable in Revvity's sole discretion, terminate this Agreement and provide a pro rata refund of any unused, prepaid fees paid by Customer (if any) for the affected Service for the subscription term remaining after the date of termination. This Section sets forth Customer's sole remedy and Revvity's entire liability in the event of any claim of infringement or misappropriation of the intellectual property rights of any third party.

(b) Indemnification of Revvity by Customer. Customer shall indemnify and defend Revvity, its affiliates, and their respective officers, agents, employees, subsidiaries, assigns, and successors in interest (collectively, "**Revvity Indemnitees**") against, and hold Revvity Indemnitees harmless from, any and all Losses awarded against Revvity Indemnitees in a final judgment resulting from any third party claim, suit, or proceeding to the extent arising from (i) Customer's violation of the terms set forth in Section 2 of this SaaS Agreement; (ii) Revvity's compliance with Customer's instructions or requests; (iii) Customer's violation of applicable data privacy laws in connection with Customer Data submitted to the Service; or (iv) Revvity's use of trademarks, Customer Data, or other materials supplied by Customer.

(c) Indemnification Procedures. If any third party makes a claim against any party who intends to seek indemnification under this Section 16, such indemnitee shall (a) promptly give written notice of such claim to the indemnifying party; (b) give the indemnifying party sole control of the defense and any settlement negotiations, provided that no settlement shall impose any obligation on any indemnitee without the prior written consent of such indemnitee; and (c) give the indemnifying party the information, authority and assistance the indemnifying party reasonably needs to defend against or settle the claim. The indemnifying party shall keep the indemnitee fully apprised at all times as to the status of the defense. Notwithstanding the foregoing, the indemnitee shall have the right to employ its own separate counsel in any such action at the sole expense of the indemnitee. Neither the indemnifying party nor any indemnitee shall be liable for the settlement of any action or claim affected without its consent.

17. EXPORT CONTROL. The Service, including Content, may be subject to the export laws and regulations of the United States and/or other jurisdictions. Neither Customer nor its Users may use, download, supply, transfer, or otherwise export or re-export the Service, except as authorized by United States law (including but not limited to the regulations administered by the U.S. Department of Commerce and the U.S. Department of the Treasury) and the laws of the jurisdiction in which the Service was obtained.

18. GOVERNMENT END USER RESTRICTION. This provision applies to software acquired directly or indirectly by or on behalf of the United States Government. The Service is a commercial product, licensed on the open market, and was developed entirely at private expense without the use of any U.S. Government funds. Use, duplication, reproduction, release, modification, disclosure, or transfer of the Service, or any related documentation, including technical data, manuals or materials, by the U.S. Government is restricted in accordance with Federal Acquisition Regulation 12.212 for civilian agencies and Defense Federal Acquisition Regulation Supplement 227.7202 for military agencies and is further restricted according to the terms of this Agreement and any amendment hereto.

19. SANCTION COMPLIANCE. (a) Customer represents and warrants that it is not located in, organized under the laws of, or owned/controlled by any person or entity subject to U.S. or applicable international sanctions and that it shall comply with all applicable economic and trade sanction laws and regulations including but not limited to U.S. Office of Foreign Asset Control, U.S. Department of Commerce Bureau of Industry and Security, the E.U. and His Majesty's Treasury of the United Kingdom (collectively "**Sanctions Laws**"). Customer shall not use the Service, directly or indirectly, in connection with any transaction or activity that would violate applicable Sanctions Laws, including providing access to the Service to any Sanctioned Party or in any Sanctioned Territory, including Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine, as such territory list may be updated by applicable Sanctions Laws. Customer shall promptly notify Revvity in writing if it becomes aware that it or any of its affiliates, employees, or agents has become subject to any sanctions designation or investigation that may affect performance under this Agreement. Revvity may terminate this Agreement, without liability or refund obligation, if Customer breaches any provision of this Section or if continued performance would cause Revvity to violate any applicable Sanctions Laws.

20. ANTI-CORRUPTION. Each party shall comply with all applicable anti-corruption and anti-bribery laws, including the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act 2010 ("UKBA"), and all other applicable national and



international anti-corruption laws (collectively, "**Anti-Corruption Laws**"). Neither party shall, directly or indirectly, offer, pay, promise, or authorize any bribe, kickback, or improper payment to any person — including any government official or private party — to obtain or retain business or secure any improper advantage. Each party shall conduct reasonable due diligence on third parties acting on its behalf in connection with this Agreement and shall ensure such third parties are bound by anti-corruption obligations no less stringent than those in this Section. Each party shall maintain accurate books and records reflecting all transactions under this Agreement, in compliance with the FCPA's accounting provisions and other applicable Anti-Corruption Laws. Each party shall promptly notify the other in writing upon becoming aware of any actual or suspected violation of this Section. Revvity may immediately terminate this Agreement, without liability or refund obligation, if Customer violates any Anti-Corruption Law in connection with this Agreement or is debarred or suspended from any government program. This Section survives expiration or termination of this Agreement for five (5) years.

21. MISCELLANEOUS.

(a) Force Majeure. Except for the obligation to pay any fees owed hereunder, neither party to this Agreement shall be responsible for any failure or delay of performance if caused by: an act of war, hostility, or sabotage; storm, blizzard, flood, or other act of God; pandemic; an electrical, internet, or telecommunication outage that is not caused by the obligated party; government restrictions or actions; or any other event outside the reasonable control of the obligated party. Each party will use reasonable efforts to mitigate the effect of a force majeure event.

(b) Independent Contractor. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, or fiduciary or employment relationship between the parties.

(c) Waiver. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right and all waivers must be affected in a writing signed by the party waiving its rights hereunder.

(d) Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the provision will be deemed null and void and shall be replaced with another term consistent with the purpose and intent of this Agreement, and the remaining provisions of this Agreement will remain in full force and effect.

(e) Notice. Any notice required under this Agreement will be provided to the other party in writing. Customer should send written notice to Revvity to: Revvity Health Sciences, Inc., 77 4th Ave, Waltham, MA 02451, USA, Attention: Legal Department with a copy to LegalNotice@Revvity.com. Revvity may give notices applicable to the Service by means of a general notice on the Service website and notices specific to Customer by electronic mail to Customer's e-mail address on record in Revvity's account information or by written communication sent by courier or first-class mail or pre-paid post to Customer's address on record in Revvity's account information. Customer shall ensure that it provides notice to Revvity of any changes in its designated contact during the term of this Agreement, and Revvity shall not be liable to Customer for any alleged failure to provide notice in the event Customer fails to provide or keep such information up to date.

(f) Assignment. Customer may not sublicense, assign, transfer the license, or give any third-party access to the Service, except as expressly authorized hereunder. Any attempt by Customer to sublicense, assign, or transfer any of the rights, duties or obligations hereunder is void. Revvity may assign this Agreement without Customer's consent in connection with a merger, acquisition or sale of all or substantially all of its assets, provided that the assignee assumes all of Revvity's obligations hereunder.

(g) Copyright Complaints and Removal Policy. Revvity does not tolerate content that appears to infringe any copyright or other intellectual property rights or otherwise violates the terms of this Agreement and will respond to notices of alleged copyright infringement that comply with the law and are properly provided to Revvity. Revvity reserves the right to delete or disable access to the Service and any content alleged to violate this Agreement and to terminate repeat infringers. Revvity's designated agent for notice of alleged copyright infringement is: Attention: Legal Department – DMCA Copyright Agent, Revvity Health Sciences, Inc., 77 4th Ave, Waltham, MA 02451 USA.

(h) Audit. Revvity may audit Customer's use of the Service (e.g., through use of software tools) to assess whether Customer's use of the Service is in accordance with the purchased subscription and the terms of this Agreement no more than one (1) audit per calendar upon thirty (30) days prior written notice, unless Revvity has reasonable cause to believe a material breach as occurred. Customer agrees to cooperate with Revvity's audit and provide reasonable assistance and access to information. Any such audit shall not unreasonably interfere with Customer's normal business operations. Customer agrees to pay any fees applicable to Customer's use of the Service in excess of Customer's rights within thirty (30) days of written notice. If Customer does not pay, Revvity can terminate Customer's access and use of the Service. Customer agrees that Revvity shall not be responsible for any of Customer's costs incurred in cooperating with the audit.

(i) Governing Law. This Agreement and all disputes arising hereunder, whether in contract, tort, or otherwise, shall be governed by and construed in accordance with the laws of the Commonwealth of Massachusetts, USA, without regard to the conflicts of law principles thereof. The United Nations Convention on Contracts for the International Sale of Goods and



the Uniform Computer Information Transactions Act do not apply to this Agreement.

(j) Entire Agreement; Modifications. This Agreement, including all addenda incorporated herein by reference and any applicable Quote, constitutes the complete Agreement between Revvity and Customer with respect to the Service and supersedes all prior or contemporaneous agreements and representations, written or oral, regarding the Service. The terms of this Agreement shall supersede the terms in any Customer purchase order, correspondence, or other similar non-Revvity document, and no terms included in any such purchase order, correspondence, or other non-Revvity document shall apply to the Service. In the event of any conflict, discrepancy, or inconsistency between this Agreement, any addenda incorporated herein by reference, or any Quote, the terms shall control in the following order: (1) the SaaS Agreement; (2) the certain, applicable Service Level Addendum (SLA) and applicable Technical Support Terms and Conditions; (3) Security Addendum; (4) Acceptable Use Policy (AUP); (5) the Cloud Service Security Addendum (Cloud Service Security Description (CSSD)); and (6) if applicable, the DPA. Except as otherwise stated in specific addenda, this Agreement shall not be amended except in an amendment, signed by an authorized representative of each party.

(k) Interpretation. The parties acknowledge that this Agreement may govern Customer's license to multiple Services offered by Revvity, if so purchased by Customer. The parties agree that the terms set forth in this Agreement shall be deemed to apply on a Service-by-Service basis. Any right or obligation of a party, including those set forth in Sections 10, 15 and 16, shall apply only in connection with the affected Service and shall not extend to any other Services purchased by Customer.

Last Updated: July 2026



SERVICE LEVEL ADDENDUM

1. **Overview.** This Service Level Addendum and any specific, additional service terms and conditions contained in the applicable product Annexes, which shall be incorporated by reference herein (“**SLA**”) governs the license and use of the Service under the terms of the Software as a Service License Agreement (“**SaaS Agreement**”) between Revvity and Customer and is subject to the terms of the SaaS Agreement. This SLA is subject to change at Revvity’s discretion, provided that such changes will not result in a material reduction in the level of availability of the Service or service credits available hereunder during the purchased subscription term. A separate annex governs service and technical support for OZ SaaS software products.
2. **Definitions.** For the purposes of this SLA, capitalized terms shall have the meanings set forth in this Section 2. Capitalized terms not otherwise defined in this Section 2 of the SLA shall have the meanings ascribed to them (i) where such capitalized term first appears in this SLA or (ii) in the SaaS Agreement.
 - 2.1 “**Availability**” or “**Available**” means, subject to the terms of this SLA, that Customer’s Users are able to access the Service.
 - 2.2 “**Actual Service Availability**” means the percentage of time that the Service was Available in the Calendar Quarter (as defined in Section 5.2) and is calculated in accordance with Section 5.2.
 - 2.3 “**Actual Uptime**” means the total number of minutes in the Calendar Quarter during which the Service was Available. Actual Uptime is measured by subtracting the total number of minutes of Unplanned Downtime in the Calendar Quarter from the total number of minutes of Scheduled Uptime in the Calendar Quarter.
 - 2.4 “**Excluded Events**” means any inability to access the Service, or any other interruption or shutdown of the Service, resulting from or due to any of the following:
 - (a) any non-scheduled emergency maintenance necessary to protect the performance, availability, stability, or security of the Service, including those initiated by Revvity in accordance with Sections 8.1-8.3 of this SLA;
 - (b) Internet congestion or slowdown, failure of the internet, or failure of Customer’s network;
 - (c) circumstances reasonably believed by Revvity (or any third-party hosting provider) to be a significant threat to the normal operation of the Service, the operating infrastructure, the facility from which the Service is provided, or otherwise relating to access to or the integrity of Customer Data (e.g., a critical vulnerability, virus, hacker, or malware or denial of service attack);
 - (d) data transmission failures outside the control of Revvity and not caused by Revvity’s negligence or willful misconduct;
 - (e) any scheduled maintenance or maintenance windows, planned outages, emergency maintenance, or unplanned downtime (i) undertaken at the request or direction of or as otherwise agreed by Customer that requires the Service to be temporarily taken offline or (ii) otherwise occurring because of any actions or omissions taken by Revvity at the request or direction of Customer;
 - (f) the failure or malfunction of Customer’s or any third party’s equipment, software components, software applications, systems, or other technology and/or integrations developed by or for Customer that are running on or interacting with the Service, in each case not solely owned or controlled by Revvity;
 - (g) system administration, commands, or file transfers performed by Customer Users or representatives;
 - (h) factors outside Revvity’s reasonable control, including, but not limited to, natural disasters, pandemics, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including Revvity’s third-party hosting provider or other vendors), and other force majeure events;
 - (i) in full or in part, any acts or omissions of Customer, its employees, contactors, agents, or any other entity over which Customer exercises control or has the right to exercise control, including negligence or material breach of Customer’s obligations under the Agreement;
 - (j) any permitted suspension or termination of Customer’s right to use the Service due to Customer’s or its Users’ breach of the SaaS Agreement, as set forth in such SaaS Agreement;
 - (k) Customer’s lack of availability or delay in responding to incidents that require Customer participation for source identification and/or resolution, including meeting Customer responsibilities for the Service;
 - (l) performance or security issues that result from Customer’s failure to accept the application of Patches made



available by Revvity;

- (m) failures or fluctuations in electrical, connectivity, network, or telecommunications equipment or lines due to circumstances outside of Revvity's reasonable control;
- (n) Customer combining or merging the Service with any hardware or software not supplied by Revvity or not identified by Revvity in the Documentation as compatible with the Service; and
- (o) any modification or changes to the configuration of any version of the Service not made by Revvity or not identified by Revvity in the Documentation.

- 2.5 **"Scheduled Downtime"** means the total number of minutes in the Calendar Quarter during which the Service is not Available due to scheduled or announced Service or system maintenance.
- 2.6 **"Scheduled Uptime"** means the total number of minutes in the Calendar Quarter, less (a) the total number of minutes of Scheduled Downtime in the Calendar Quarter and (b) the total number of minutes in which the Service is not Available due to any or all Excluded Events occurring during such Calendar Quarter.
- 2.7 **"Unplanned Downtime"** means the total number of minutes in the Calendar Quarter during which the Customer had complete loss of ability to access the Service, excluding Scheduled Downtime and any time during which the Service or any Service component is not Available due to an Excluded Event. Unplanned Downtime will be calculated beginning on the second consecutive detection of Unplanned Downtime within a five-minute period and will end when the unplanned downtime has been resolved, in each case as detected by Revvity's internal monitoring systems.
- 3. **Hours of Operation.** Revvity will use commercially reasonable efforts to make the Service Available to Customer 24 hours a day, 7 days a week, 365 days a year, except during Scheduled Downtime, Excluded Events, and as otherwise set forth in the SaaS Agreement and this SLA.
- 4. **Service Access; Network Bandwidth and Latency.** Customer access to the Service is through the Internet. Revvity is not responsible for Customer's network connections or for conditions or problems arising from or related to Customer's network connections (e.g., bandwidth issues, excessive latency, network outages) or caused by the Internet. Revvity monitors Service Availability 24/7/365 by utilizing its own internal monitoring systems. Revvity will notify Customers of any identified issues that will impact Service Availability as soon as practicable via email to Customer's designated point of contact.
- 5. **Service Availability.**
 - 5.1 **Service Availability Target.** Except as otherwise set forth in the Quote, Revvity will use commercially reasonable efforts to make the Service Available for a Calendar Quarter uptime percentage of 99.5% (the **"Service Availability Target"**).
 - 5.2 **Calculation of Actual Service Availability.** Measurement of Actual Service Availability begins on the date that the production environment for the Service has been made available for access by Customer in accordance with Revvity's standard business process. Following the end of each of calendar quarter of the purchased subscription term (January – March; April – June; July – September; October – December) (each, a **"Calendar Quarter"**), Revvity measures the Actual Service Availability by dividing the Actual Uptime by the Scheduled Uptime and multiplying by 100. All Scheduled Downtime and Unplanned Downtime will be rounded up or down to the nearest one-minute increment, with increments equal to or greater than thirty (30) seconds being rounded up to the next minute. Final determinations of the length of the cumulative periods of Scheduled Downtime and Unplanned Downtime over a Calendar Quarter shall be based on Revvity's internal server monitoring equipment and records.
- 6. **Reporting.** Customer may request a report detailing the Service Availability (**"Availability Report"**) within fifteen (15) days of the end of the prior Calendar Quarter by sending such request to its regional Revvity Technical Support team. Any claims relating to the accuracy of the Availability Report shall be deemed waived if notice of such dispute is not received within fifteen (15) days of the date Revvity provides such Availability Report to Customer. Revvity shall be the final arbiter of all determinations of Actual Service Availability and failure to meet the Service Availability Target in accordance with this SLA.



7. **Disaster Recovery Capabilities.** Revvity will provide disaster recovery capabilities to restore the Service in the event the Service is completely down. Customer Data images are created for disaster recovery purposes only. "Recovery Point Objective" or "RPO" means the maximum acceptable level of data loss following an unplanned event, such as a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data). Revvity's RPO is 24 hours. "Recovery Time Objective" or "RTO" means the period of time within which Service must be restored following an unplanned event or disaster. Revvity's RTO is 48 hours.
8. **Service Maintenance and Change Management Policy.**
 - 8.1 **Service Maintenance and Changes.** Revvity performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the Service. For changes that are expected to cause service interruption, Revvity will endeavor to provide prior notice of the anticipated impact. For Customer-specific changes and upgrades, Revvity will work to coordinate the maintenance periods with Customer where possible. The durations of the maintenance periods for scheduled or planned maintenance are not included in the calculation of Unplanned Downtime minutes in the quarterly measurement period for Service Availability. Revvity uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that may cause Service interruptions.
 - 8.2 **Emergency Maintenance.** Revvity may periodically be required to execute emergency maintenance to protect the security, performance, availability, or stability of the Service. Emergency maintenance may include program patching and/or core system maintenance, as required. Revvity will work to minimize the use of emergency maintenance and, where reasonably practicable, will endeavor to provide Customer prior notice of any emergency maintenance requiring a service interruption.
 - 8.3 **Major Maintenance Changes.** To help ensure continuous stability, availability, security, and performance of the Service, Revvity reserves the right to perform major changes to its hardware infrastructure, operating software, applications software, and supporting application software under its control. Each such change event is considered planned maintenance and may cause the Service to be unavailable for up to twenty-four (24) hours. Revvity will endeavor to provide planned maintenance outside of the hours of 8:00AM to 5:00pm EST (for customers in the United States) and 9:00AM to 5PM EET (for customers outside the United States). Revvity will endeavor to provide prior notice of the anticipated unavailability.
 - 8.4 **Software version updates.** Revvity shall be responsible to maintain only the current version of the Service. In the event of a new version release of the Services, Revvity will provide notice of at least seven (7) days prior to the effective date of the Service's new version. Services shall automatically update to the latest version, without requiring Customer's prior consent.
9. **Support Fees.**
 - 9.1 **Support Fees.** The fees paid by Customer for the Service include Revvity's provision of the technical support services described in this SLA ("Support Fees"). Additional fees are applicable for any other Revvity support service offerings or other professional or consulting services purchased by Customer.
 - 9.2 **Support Period.** Technical Support (as defined below) becomes available on the start date of the Service subscription term and ends upon the expiration or termination of the Service subscription term set forth in the applicable Quote. Revvity is not obligated to provide the Technical Support described in this SLA beyond the end of the purchased Service subscription term.
 - 9.3 **Customer Responsibilities.** Revvity's obligation to provide support is contingent upon the Customer complying with the following conditions:
 - (a) Paying the mutually agreed upon support fees;



- (b) Provide Revvity with sufficient information and resources to correct all support issues;
- (c) Obtain Revvity's written permission prior to performing or attempting to perform modifications to the System (Revvity shall not be responsible for maintaining Customer modified portions of the System or for maintaining portions of the System affected by Customer modified portions of the System);
- (d) Comply with Revvity's "Software Deployment Terms and Conditions" regarding support services; and
- (e) Customer shall also nominate System Owner. System Owner is the liaison between Customer and Revvity for Technical Support and will be responsible for communicating with and providing timely and accurate information and feedback to Revvity in connection with the Technical Support. Customer's contacts must be knowledgeable about the Service and the environment to help resolve service issues and to assist Revvity in analyzing and resolving Technical Support requests. When submitting a Technical Support request, Customer's technical contact should have a baseline understanding of the problem being encountered and an ability to reproduce the problem to assist Revvity in diagnosing and triaging the problem. To avoid interruptions in Technical Support, Customer must notify Revvity whenever technical contact responsibilities are transferred to another individual.

Last Updated: July 2026



ANNEX: SERVICE LEVEL ADDENDUM FOR OZ SAAS PRODUCTS

1. **Overview.** The terms and conditions of this Service Level Addendum (“SLA”) applies to Revvity’s OZ SaaS products (the “Service”) and modules and governs the Technical Support (as defined herein) provide to Customer for such product(s). This SLA is subject to change at Revvity’s discretion, provided that such changes will not result in a material reduction in the level of the availability of the Service.
2. **Definitions.** For the purposes of this SLA, capitalized terms shall have the meanings set forth in this Section 2. Capitalized terms not otherwise defined in this SLA shall have the meanings ascribed to them in the Agreement.
 - 2.1. **“Available”** means, subject to the terms of this SLA, that Users are able to access the Service.
 - 2.2. **“Excluded Events”** means any inability to access the Service, or any other interruption or shutdown of the Service, resulting from or due to any of the following:
 - a) any non-scheduled emergency maintenance necessary to protect the performance, availability, stability, or security of the Service, including those initiated by Revvity in accordance with Sections 5.1-5.3 of this SLA;
 - b) Internet congestion or slowdown, failure of the internet, or failure of Licensee’s network;
 - c) circumstances reasonably believed by Revvity (or any third-party hosting provider) to be a significant threat to the normal operation of the Service, the operating infrastructure, the facility from which the Service is provided, or otherwise relating to access to or the integrity of Licensee Data (e.g., a critical vulnerability, virus, hacker, or malware or denial of service attack);
 - d) data transmission failures outside the control of Revvity and not caused by Revvity’s negligence or willful misconduct;
 - e) any scheduled maintenance or maintenance windows, planned outages, emergency maintenance, or unplanned downtime (i) undertaken at the request or direction of or as otherwise agreed by Licensee that requires the Service to be temporarily taken offline or (ii) otherwise occurring because of any actions or omissions taken by Revvity at the request or direction of Licensee;
 - f) the failure or malfunction of Licensee’s or any third party’s equipment, software components, software applications, systems, or other technology and/or integrations developed by or for Licensee that are running on or interacting with the Service, in each case not solely owned or controlled by Revvity;
 - g) system administration, commands, or file transfers performed by Licensee’s Authorized Users or representatives;
 - h) factors outside Revvity’s reasonable control, including, but not limited to, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including Revvity’s third-party hosting provider or other vendors), and other force majeure events;
 - i) in full or in part, any acts or omissions of Licensee, its employees, contactors, agents, or any other entity over which Licensee exercises control or has the right to exercise control, including negligence or material breach of Licensee’s obligations under the Agreement;
 - j) any permitted suspension or termination of Licensee’s right to use the Service due to Licensee’s or its Authorized Users’ breach of the Agreement, as set forth in such Agreement;
 - k) Licensee’s lack of availability or delay in responding to incidents that require Licensee participation for source identification and/or resolution, including meeting Licensee responsibilities for the Service;
 - l) performance or security issues that result from Licensee’s failure to accept the application of Patches made.
3. **Hours of Operation.** Revvity will use commercially reasonable efforts to make the Service available to Licensee 24 hours a day, 7 days a week, 365 days a year, except during scheduled downtime, Excluded Events, and as otherwise set forth in the Agreement and this SLA.
4. **Service Access; Network Bandwidth and Latency.** Licensee’s access to the Service is through the Internet. Revvity is not responsible for Licensee’s network connections or for conditions or problems arising from or related to Licensee’s network connections (e.g., bandwidth issues, excessive latency, network outages) or caused by the Internet. Revvity



will notify Licensee of any identified issues that will impact Service Availability as soon as practicable via email to Licensee's designated point of contact or a recorded message on the customer support line.

5. Service Maintenance and Change Management Policy.

5.1. Service Maintenance and Changes. Revvity performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the Service. For changes that are expected to cause service interruption, Revvity will endeavor to provide prior notice of the anticipated impact. For Licensee-specific changes and upgrades, Revvity will work to coordinate the maintenance periods with Licensee where possible. The durations of the maintenance periods for scheduled or planned maintenance are not included in the calculation of Unplanned Downtime minutes in the quarterly measurement period for Service Availability. Revvity uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that may cause Service interruptions. All relevant Service notifications will be posted on the homepage located within the purchased Service.

5.2. Emergency Maintenance. Revvity may periodically be required to execute emergency maintenance to protect the security, performance, availability, or stability of the Service. Emergency maintenance may include program patching and/or core system maintenance, as required. Revvity will work to minimize the use of emergency maintenance and, where reasonably practicable, will endeavor to provide Licensee prior notice of any emergency maintenance requiring a service interruption.

5.3. Major Maintenance Changes. To help ensure continuous stability, availability, security, and performance of the Service, Revvity reserves the right to perform major changes to its hardware infrastructure, operating software, applications software, and supporting application software under its control. Each such change event is considered planned maintenance and may cause the Service to be unavailable for up to twenty-four (24) hours. Revvity will endeavor to provide prior notice of the anticipated unavailability.

6. Technical Support. The fees paid by Licensee for the Service (the "License Fees") of the Agreement include Revvity's provision of the technical support services described in Section 7 of this SLA ("**Technical Support**"). Additional fees are applicable for any other Revvity support service offerings or other professional or consulting services purchased by Licensee. Technical Support becomes available on the start date of the Service subscription term and ends upon the expiration or termination of the Service subscription term set forth in the applicable Quote. Revvity is not obligated to provide the Technical Support described in this SLA beyond the end of the Term of the Agreement.

7. "Technical Support**"** includes the following, as may apply for the applicable Service licensed to Licensee under the Agreement:

Service	Description of Technical Support Services
Telepathy EHDI	• Software updates • Provide support for hardware changes (i.e. laptop) • Access to customer support, 365 days/year, 8:00AM to 5:30PM CST via email (oz.help@revvity.com) or telephone (888.727.3366)
Telepathy CCHD	• Software updates • Provide support for hardware changes (i.e. printer, laptop, pulse oximeter) • Access to customer support, 365 days/year, 8:00AM to 5:30PM CST via email (oz.help@revvity.com) or telephone (888.727.3366) • Provide monthly reports for the first 3 months post implementation on program performance • Provide a year-end report containing 12-month performance • Provide a monthly report, upon request
Telepathy NBS	• Software updates • Update e-form and label print outs in response to new state specimen card requirements



	• Test and monitor electronic lab orders to the state laboratory • Provide support for hardware changes (i.e. printer, laptop) • Access to customer support, 365 days/year, 8:00AM to 5:30PM CST via email (oz.help@revvity.com) or telephone (888.727.3366) • Provide monthly reports for the first 3 months post implementation on program performance • Provide a year-end report containing monthly performance • Provide a monthly report, upon request
HL7 Message Interfaces (OZ NANI and OZ Connect EHDI, CCHD & NBS Results back to EHR)	• Monitor and provide alerts regarding the message feed • Maintain VPN tunnel used for interface communications • Update interface to improve security and enhance the interface • Notify of scheduled downtime • Notify if unexpected downtime occurs due to system outages • Work with hospital IT department on any requested hospital interface maintenance projects • Electronic health record system or interface engine migrations

Last Updated: July 2026



ACCEPTABLE USE POLICY

Overview: This Acceptable Use Policy (“AUP”) outlines acceptable uses of Revvity Health Sciences, Inc.’s (together with its affiliates, “**Revvity**”) software as a service offerings (collectively for the purposes of this policy, the “**Services**”) and is incorporated by reference into the Software as a Service Licensing Agreement, to which this is attached and referenced, governing its use of the Service(s) (“**Agreement**”). This AUP prohibits uses and activities involving the Services that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Services by others. Revvity reserves the right to change or modify the terms of this AUP from time to time, effective when posted on Revvity’s website (the “**Site**”). Revvity will endeavor to provide Customer’s with notice of material change to this AUP; *provided however*, that Customer’s use of the Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms. Any capitalized terms not otherwise defined in this AUP shall have the meaning ascribed to them in Customer’s Agreement.

Prohibited Uses:

1. **Unlawful Activities:** The Services shall not be used in violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. This includes, but is not limited to:
 - a) Child pornography
 - b) Unlawful gambling activities
 - c) Threats, harassment, or abuse of any individual, organization or business
 - d) Fraudulent activities
 - e) Terrorist websites or other sites advocating human violence or hate crimes based upon race, religion, ethnicity, country of origin, political opinion, sex, gender, sexual orientation or identity, gender identity, or any other protected class
 - f) Unlawful high yield investment plans, Ponzi schemes, or linking to or advertising such schemes.
2. **Pornography:** The Services shall not be used to publish, submit, receive, upload, download, post, use, copy or otherwise produce, transmit, distribute or store pornography.
3. **Unsolicited Email:** The Services shall not be used to send or receive mass unsolicited email (“**SPAM**”). This prohibition includes the direct or indirect sending and receiving of such messages, support of such messages via web page, splash page, or other related sites, or the advertisement of such services. The falsifying of packet header, sender, or user information, in whole or in part, to mask the identity of the sender, originator, or point of origin, or knowingly deleting any author attributions, legal notices, proprietary designations, or labels in a file that the Customer mails or sends is expressly prohibited.
4. **Email Bombing:** The Services shall not be used for sending, returning, bouncing, or forwarding email to specified user(s) in an attempt to interfere with or overflow email services.
5. **Proxy Email:** The Services shall not be used as a proxy email server to forward email to unrelated third parties.
6. **UseNet SPAM:** The Services shall not be used to send, receive, forward, or post UseNet unsolicited email or posts. This includes UseNet services located within the Revvity network.
7. **Hacking:** The Services shall not be used for hacking, attacking, gaining access to, breaching, circumventing, or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software, or data without the express authorization of the owner of the system or network.
8. **Threatening Material or Content:** The Services shall not be used to host, post, transmit, or retransmit any content or material that harasses or threatens the health or safety of others. In addition, Revvity reserves the right to decline



to provide Services if Customer's use is determined by Revvity in its sole reasonable discretion to be obscene, indecent, vulgar, abusive, hateful, malicious, racist or otherwise promoting bigotry, defamatory, fraudulent, libelous, treasonous, tortious, excessively violent or promoting the use of violence, or otherwise harmful to others.

9. **Violation of Intellectual Property Rights:** The Services shall not be used to publish, submit, receive, upload, download, post, use, copy or otherwise reproduce, transmit, retransmit, distribute, or store any content or material or to engage in any activity that infringes, misappropriates, or otherwise violates the intellectual property rights or publicity rights of Revvity or any third party, including but not limited to any rights protected by any copyright, patent, trademark, trade secret, trade dress, right of publicity, moral rights, or other intellectual property right now known or later recognized by statute, judicial decision or regulation.
10. **Violation of Privacy Rights:** The Services shall not be used to violate any individual's privacy rights and all use of the Services shall comply with all applicable privacy laws and regulations applicable to the use of the Service or Customer Data.
11. **Distribution of Malware:** The Services shall not be used for the storage, distribution, fabrication, or use of malware, including without limitation virus software, worms, Trojan horses, root kits, password crackers, adware, key stroke capture programs, or other programs normally used in malicious activity. The use of such programs in the ordinary course of business, however, may be requested by Customer and approved by Revvity on a case-by-case basis.
12. **Phishing:** The Services shall not be used for any activity designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email, or any activity related to phishing activities may result in the immediate suspension of Customer's account.
13. **Server Abuse:** Abuse or excessive use of Revvity's servers, network, and infrastructure is prohibited, including but not limited to data scraping or data training.
14. **Network Abuse:** Any activity that involves making network connections to any third party without permission is prohibited. Such activity includes, but is not limited to, intentional network interference, port scanning, monitoring, crawling, denial of service, network penetration, sniffing, spoofing, virus deployment, hack attempts, vulnerability scanning, and avoidance of third-party network security restrictions or limitations.
15. **Security Abuse:** Any activity that involves violating the security or integrity of any Revvity network, system, application, device or other technology, account, password protection, or computer is prohibited. Such activity includes, but is not limited to, unauthorized access, internet scamming, password robbery, spidering, harvesting, collection of e-mail addresses or other identifiers, probing, scanning, penetrating, testing, interception, monitoring, network, packet header or e-mail origin falsification (excluding proper use of aliases), covert user information gathering, or otherwise trying to breach the security of Revvity's network, system, applications, or other security features.
16. **Vulnerability Testing:** Customer may not perform any kind of vulnerability testing, penetration testing, or network scans, whether by passive or intrusive techniques, to test the vulnerability of any Revvity system or Revvity's network without Revvity's express written consent.

Reporting Violations of the Acceptable Use Policy. Revvity accepts reports of alleged violations of this AUP via email. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, the IP address or website allegedly in violation, and a description of the alleged violation. Unless otherwise required by law, such as the DMCA, Revvity owes no duty to third parties reporting alleged violations. Revvity will review all verified third-party reports and will take such actions as it deems appropriate in its reasonable discretion. Revvity will comply with and respond to valid (as Revvity determines in its reasonable discretion) subpoenas, warrants, or court orders. If permitted by applicable law or regulation, Revvity may forward such subpoenas, warrants, or orders to Customer and Customer



may respond; however, Revvity reserves the right to respond to any such subpoena, warrant or order if it is the named party in such subpoena, warrant, or order.

Violations and Revvity's Rights. Revvity reserves the right, but does not assume the obligation, to investigate any violation of this AUP. Revvity will act as the sole arbiter as to what constitutes a violation of this AUP. At any time after a violation has occurred, and during the time that any violation is being investigated, Revvity reserves the right to suspend, restrict, or terminate any Services at any time, including without limitation the "blackholing" or "suspension" of suspected IP addresses or hosts, without liability to Customer, in accordance with the terms of the Agreement.

Last Updated: July 2026



SECURITY AND PRIVACY ADDENDUM

OVERVIEW. Revvity (together with its affiliates, “**Revvity**”) has designed this Security and Privacy Addendum (“**Security and Privacy Addendum**”) to protect the confidentiality, integrity, availability, and privacy of Customer Data, taking into account the type of Service being provided, the resources available to Revvity, the nature of Customer Data being input into the Services, and Revvity’s commitment to protecting the security and privacy of such Customer Data.

This Security and Privacy Addendum is subject to change at Revvity’s discretion, provided that such changes will not result in a material reduction in the security level of the Service provided during the purchased subscription term.

1. DEFINITIONS. All capitalized terms not otherwise defined herein shall have the meanings ascribed to them in applicable Software as a Service License Agreement (“**SaaS Agreement**”).

“**Affiliate**” means any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the Party. For purposes of this definition, the term “control” means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

“**Applicable Law**” means any international, foreign, national, federal, state, or local statutes, ordinances, regulations, rules, executive orders, supervisory requirements, directives, circulars, opinions, judgments, interpretive letters, official releases, and other pronouncements having the effect of law and requirements or standards issued by a self-regulatory organization which apply from time to time to the person or activity in the circumstances in question. Applicable Law includes any of the foregoing as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

“**CCPA**” means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

“**Colorado CPA**” means the Colorado Consumer Privacy Act of 2021 (Col. Rev. Stat. 6-1-13 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

“**Controller**” means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the Party that, alone or jointly with others, determines the means and purpose of the Processing of Personal Data. Without limiting the foregoing, the term “Controller” includes a “business” under the CCPA or CPRA.

“**CPRA**” means the California Consumer Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

“**Data Protection Laws**” means any Applicable Law relating to Personal Data or collection, use, storage, disclosure, transfer, or other Processing of Personal Data of or by any government, or any authority, department, or agency thereof, or self-regulatory organization, including, without limitation: (a) GDPR; (b) UK GDPR; (c) LGPD; (d) CCPA; (e) PIPEDA; (f) CPRA (when in effect); (g) Virginia CDPA (when in effect); and (h) Colorado CPA (when in effect).

“**Data Subject**” means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the individual who is the subject of Personal Data that Revvity Processes for Customer. Without limiting the foregoing, the term “Data Subject” includes a “consumer” as defined under the CCPA or CPRA.



"EU Standard Contractual Clauses" or **"EU-SCCs"** means the applicable module(s) of the European Commission's standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as set out in the Annex to Commission Implementing Decision (EU) 2021/914, a completed copy of which comprises Exhibit 1, as amended, supplemented, or otherwise modified from time to time.

"GDPR" means the EU General Data Protection Regulation (EU Regulation 2016/679) and the implementing acts of the foregoing by a Member State, Switzerland, each as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"Member State" means a member state of the European Union and/or the European Economic Area, as may be amended from time to time.

"Personal Data" means any information Revvity Processes for Customer (other than contact information for Customer or Customer's personnel) that: (a) the relevant Data Protection Laws otherwise define as "personal information" or "personal data."; or (b) in absence of such a definition in the relevant Data Protection Laws, such information that identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Revvity's possession or control or that Revvity is likely to have access to. Without limiting the foregoing, the term "Personal Data" includes any "personal data" as defined under the GDPR and any "personal information" as defined under the CCPA and the CPRA. Without limiting the foregoing, Personal Data includes the Data Subject's name, an identification number, geo-location data, an online user identification.

"PIPEDA" means the Canadian Personal Information Protection and Electronics Documents Act, as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"Process" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring Personal Data to third parties. The terms **"Processing"** and **"Processed"** have a correlative meaning.

"Processor" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the Party that Processes the Personal Data on behalf of the Controller. Without limiting the foregoing, the term "Processor" includes a "service provider" or a "contractor" under the CCPA or CPRA.

"Security Incident" means any act or omission that materially compromises or is reasonably likely to materially compromise either the confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organizational safeguards put in place by Revvity, that relate to the protection of the confidentiality, integrity, or availability of Personal Data. Without limiting the foregoing, a material compromise includes any accidental, unlawful, or unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Personal Data. Notwithstanding the foregoing, the term "Security Incident" does not include any event that does not result in any unauthorized access to Personal Data or to Revvity's equipment or facilities storing Personal Data, including, without limitation, pings and other broadcast attacks on firewalls or other network equipment, port scans, unsuccessful logon attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond communication headers) or similar incidents.

"Standard Contractual Clauses" means the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, as applicable.



"Subprocessor" means a third-party engaged by Revvity to assist with the provision of the Services which involves the Processing of Personal Data.

"UK GDPR" means the United Kingdom Data Protection Act of 2018 and the United Kingdom General Data Protection Act, as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"UK Standard Contractual Clauses" or **"UK-IDTA"** means the International Data Transfer Addendum ("IDTA") to the EU Standard Contractual Clauses, issued by the UK Information Commissioner's Office ("ICO") pursuant to Section 119A of the Data Protection Act 2018, for the transfer of Personal Information from the United Kingdom to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, as may be amended, modified, or replaced by the United Kingdom, a completed copy of which comprises Exhibit 2, as amended, supplemented or otherwise modified from time to time.

"Virginia CDPA" means the Virginia Consumer Data Protection Act of 2021 (Virginia Code § 59.1-571 et seq.).

2. **RELATIONSHIP WITH LICENSE AGREEMENT.** If Customer is a party to the Agreement, this Security and Privacy Addendum is subject to the terms of the SaaS Agreement and is hereby incorporated into the SaaS Agreement. If Customer has executed an Order with Revvity pursuant to the Agreement, but is not itself a party to the Agreement, then this Security and Privacy Addendum is an addendum to that Order and all applicable renewal Orders. All related exhibits, schedules, attachments, appendices, and any other documents incorporated herein by reference (collectively, the "Addendum") form part of this Security and Privacy Addendum and will have effect as if set out in full in the body of this Security and Privacy Addendum. Any reference to this Security and Privacy Addendum includes such Addendum. Notwithstanding anything to the contrary in the SaaS Agreement, in case of a conflict, inconsistency, or ambiguity between the Standard Contractual Clauses, the Addendum, and the body of this Security and Privacy Addendum, the following order of precedence governs: (a) first, the Standard Contractual Clauses; (b) second, the body of this Security and Privacy Addendum (to the extent this Security and Privacy Addendum requires additional, more stringent, or more protective obligations than the Addendum or the SaaS Agreement); (c) third, the Addendum; and (d) fourth, the SaaS Agreement.
3. **RELATIONSHIP OF THE PARTIES.** Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including providing any required notices and obtaining any required consents (except to the extent explicitly set forth in the SaaS Agreement), and for the Processing instructions it gives to Revvity. The Parties acknowledge and agree that with regard to the Processing of Personal Data (other than contact information of Customer or Customer's personnel, for which the Parties are independent controllers), Revvity is the "Processor" and Customer is the "Controller" under this agreement.
4. **CUSTOMER OBLIGATIONS.**
 - 4.1. **Compliance with Laws.** Customer shall, in its use of the Services, Process the Personal Data in accordance with the requirements of applicable Data Protection Laws.
 - 4.2. **Licenses and Registrations.** Customer shall obtain all material licenses, authorizations, approvals, consents, or permits required of it as a Controller under applicable Data Protection Laws to Process the Personal Data as set forth in this Security and Privacy Addendum, the SaaS Agreement, or as required under Data Protection Laws and to perform its obligations under this Security and Privacy Addendum or the SaaS Agreement.
 - 4.3. **Customer Instructions.** Customer's instructions to Revvity for the Processing of Personal Data will comply with Data Protection Laws and Customer will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.



4.4. Data Protection Officers and Representatives. To the extent required by applicable Data Protection Laws, Customer shall appoint data protection representative and/or data protection officers in all applicable jurisdictions.

5. REVVITY'S OBLIGATIONS.

5.1. Scope of Processing. The nature, scope, and purpose of the Processing of Personal Data is set forth in Appendix A.

5.2. Compliance with Data Protection Laws. Revvity will comply in all material respects with applicable Data Protection Laws with respect to its Processing of Personal Data and provision of the Services.

5.3. Licenses and Registrations. Revvity shall obtain all material licenses, authorizations, approvals, consents or permits required of it as a Processor under applicable Data Protection Laws to perform its obligations and Process the Personal Data under this Security and Privacy Addendum and the SaaS Agreement.

5.4. Data Protection Officers and Representatives. To the extent required by applicable Data Protection Laws, Revvity shall appoint one or more data protection representatives and/or data protection officers in the applicable jurisdictions.

5.5. Limited Processing; Confidentiality. Revvity agrees and covenants that it shall: (a) not create, collect, receive, access, use, or otherwise Process the Personal Data in violation of any Applicable Law (including Data Protection Laws); (b) Process the Personal Data solely and exclusively for the purposes for which the Personal Data, or access to it, is provided pursuant to the terms and conditions of the SaaS Agreement and this Security and Privacy Addendum; and (c) not collect, retain, use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Data outside of the direct business relationship with Customer or for Revvity's own purposes or for the benefit of anyone other than Customer's, in each case, without Customer's prior written consent. Notwithstanding the foregoing, unless explicitly prohibited by Customer in writing (including under the SaaS Agreement or this Security and Privacy Addendum), Revvity may use the Personal Data as follows to the extent permitted by applicable Data Protection Laws: (i) internal use of anonymized data to build or improve the quality of the Services provided by Revvity, provided, however, that Revvity does not use the Personal Data to build or modify a profile about a Data Subject or their household to use in providing services to a third-party, or cleaning or augmenting any Personal Data acquired from another source; (ii) to detect Security Incidents, or to protect against fraudulent or illegal activity; (iii) as otherwise explicitly permitted under Data Protection Law; and (iv) to respond to any Legal Order.

5.6. Instructions from Customer. Revvity shall only Process the Personal Data to the extent, and in such a manner, as is necessary to perform the Services in accordance with Customer's documented instructions. Customer may provide Revvity with general or specific data protection-related instructions. Revvity shall not Process the Personal Data for any other purpose or in a way that does not comply with this Security and Privacy Addendum or the Data Protection Laws. To the extent permitted by Applicable Law, Revvity shall promptly notify Customer if, in its reasonable opinion, Customer's instruction would not comply with the Data Protection Laws. Without limiting the foregoing, Customer hereby instructs Revvity to Process the Personal Data for the following purposes: (a) as necessary for the provision of the Services and in accordance with this Security and Privacy Addendum and the SaaS Agreement; (b) as initiated by Customer's end users in their use of the Services; (c) to comply with other reasonable instructions provided by Customer to Revvity (e.g., via email or via support requests) where such instructions are consistent with the terms of the SaaS Agreement and this Security and Privacy Addendum; and (d) to respond to a Legal Order.

5.7. Excess Processing Requirements. In the event Revvity is required under any applicable Data Protection Law to Process the Personal Data in excess of Customer's documented instructions, Revvity shall immediately notify



Customer of such a requirement, unless such applicable Data Protection Law prohibits such notification, in which case Revvity shall notify Customer of this required Processing as soon as the applicable Data Protection Law permits it to do so.

5.8. Inability to Comply. Revvity shall promptly inform Customer in the event Revvity cannot reasonably provide compliance with this Security and Privacy Addendum for whatever reason. In such an event, Customer may immediately suspend any Processing of Personal Data and/or terminate the Services pursuant to the SaaS Agreement.

5.9. Assistance in Compliance with Obligations under Data Protection Laws. Taking into account the nature of Revvity's Processing and the information available to Revvity, Revvity shall reasonably assist Customer in meeting Customer's compliance obligations under the Data Protection Laws (including, without limitation, Customer's security requirements, notifications or other communications related to any Security Incidents, responding to Data Subject Requests, and any data privacy impact assessments and/or prior consultations with supervisory authorities or other competent data privacy authorities provided for under applicable Data Protection Laws) through appropriate technical and organizational measures. Revvity reserves the right to invoice, and Customer shall pay, for any additional costs arising from Revvity's provision of such assistance.

5.10. Cooperation with Regulators. At Customer's sole cost and expense, Revvity and its representatives shall cooperate, upon request from Customer, with any and all requests from data protection authorities and regulators having jurisdiction over Customer, including those with jurisdiction to monitor and ensure compliance with applicable Data Protection Laws.

5.11. Requests from Customer. Revvity shall promptly comply with any Customer request or instruction requiring Revvity to amend, transfer, delete, or perform any other lawful Processing of Personal Data, and to stop, mitigate, or remedy any unauthorized Processing.

5.12. Data Analytics; Anonymized Personal Data. Any data collected pursuant to data analytics or monitoring carried out by Revvity in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data. Revvity may aggregate, de-identify, or anonymize Personal Data and use such aggregated, de-identified, or anonymized data, which shall no longer be considered Personal Data, for its own reasonable purposes. Customer hereby authorizes Revvity to Process the Personal Data for the purposes described in this Section 5.12.

6. COMPLAINTS; DATA SUBJECT REQUESTS; AND THIRD PARTY RIGHTS.

6.1. Complaints and Other Communication. Revvity shall notify Customer in the event it receives any request, complaint, or communication relating to Customer's obligations under Data Protection Laws (including from data protection authorities and/or supervisory authorities). To the extent permitted by applicable Data Protection Laws, Revvity shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.

6.2. Data Subject Requests Received by Revvity. Revvity shall, to the extent permitted under Applicable Law, promptly notify Customer if Revvity receives a request from a Data Subject or their representative to exercise any rights provided to Data Subject with respect to their Personal Data under applicable Data Protection Laws, including, but not limited to, any rights of access, rectification, erasure, data portability, or restriction of Processing, right to object to Processing, right to not have their Personal Data shared or sold, or not to be subject to automated decision making ("Data Subject Request").

6.3. Assistance with Data Subject Requests. Taking into account the nature of the Processing, Revvity shall provide all reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is



possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws. The parties agree and acknowledge that Revvity may, but is not required to, fulfill its obligations described in the foregoing sentence by providing Customer with access to features and functions of the Services such that Customer can fulfill the Data Subject Request without assistance from Revvity. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Revvity shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Revvity is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Revvity's provision of such assistance.

7. CONFIDENTIALITY.

7.1. Revvity's Personnel. Unless otherwise required by law, Revvity shall keep and maintain all Personal Data in strict confidence, using such a degree of care as is appropriate to avoid unauthorized access, use or disclosure (taking into account the state of the art, costs and implementation, and the nature, scope, context, and purposes of the Processing as well as the risks to the rights of Data Subjects). Unless otherwise required by Applicable Law, Revvity shall not disclose or permit access to the Personal Data other than to its employees, officers, directors, attorneys, and agents who need to know or access the Personal Data to meet Revvity's obligations under this Security and Privacy Addendum and the SaaS Agreement (each, a "**Revvity Representative**"). Revvity shall require that such Revvity Representatives: (a) are informed of the confidential nature and use restrictions regarding the Personal Data; and (b) have committed themselves to maintaining the confidentiality of the Personal Data or are under an appropriate statutory obligation of confidentiality.

8. SECURITY MEASURES.

8.1. Security Practices. Revvity is responsible for implementing and maintaining the technical, process, and organizational security measures in relation to the Service set forth in this Security and Privacy Addendum. Revvity provides system administrator rights to Customer, but Customer is responsible for managing secure practices regarding user access as described in Section 8.5. Customer remains the primary account and system administrator and is responsible for security, maintenance, and appropriate protection of Customer Data by (i) selecting and purchasing appropriate Service(s), (ii) implementing appropriate identity, encryption and logical access controls, and (iii) implementing and ensuring compliance with any Customer-specific security measures implemented by Customer for the use of the Service by its Users. Certain Revvity services may be available to help Customer meet these requirements. Customer may contact its Revvity Sales Account Representative for further details. Any data exported from the system is responsibility of the Customer.

8.2. Physical Security. Revvity utilizes public cloud infrastructure, including Amazon Web Services, as third-party service providers in connection with its provision of the Service. The following physical security controls apply to the Service, and may, as applicable, be performed by Revvity's third-party service providers:

- a) Revvity's third-party service providers provide the servers utilized in Revvity's provision of the Service, are responsible for the physical security of the data centers, and are either SSAE18-SOC 2 Type 2 certified or have been reviewed by Revvity to ensure conformance by such service provider to the requirements of the Trust Services Criteria of Security, Availability, and Confidentiality published by the American Institute of Certified Public Accountants.
- b) Revvity's third-party hosting providers are required to maintain controls and periodically review access to the data centers utilized by Revvity Health Sciences, including, but not limited to, controls such as badge access and video monitoring. Revvity additionally reviews and monitors physical access control enforcement.

8.3. Security Controls Audit and Reporting. Revvity will engage qualified third-party auditors to perform annual examinations of its systems and processes related to the Service. A Revvity ISO/IEC 27001 certificate or equivalent report (as determined by Revvity) may be available to Customer upon Customer's request, subject



to Revvity's document distribution requirements. Any document provided by Revvity to Customer shall be deemed Revvity Confidential Information and subject to the confidentiality obligations set forth in the SaaS Agreement or other confidentiality agreement entered into by and between the parties, as applicable.

8.4. Administrative controls.

8.4.1. Screening. Revvity will perform pre-employment background screening, under applicable laws, on employees and contractors who have access to Customer accounts.

8.4.2. Revvity Access. Revvity will restrict access to Customer accounts to its employees, contractors, and agents who require access for the sole purpose of providing the Service (including the provision of professional and technical support services during the subscription term), subject to need and least privilege principles. Revvity personnel who access the Service will be required to log on using an assigned username and password and are required to complete appropriate security, data classification, and privacy training. Further, administrative access granted to employees, contractors, and agents will be reviewed periodically to determine the appropriateness of access based on his or her role and relationship with Revvity.

8.5. Customer Access. As the primary administrator of the Service, Customer is responsible for the management of its end user accounts, including creation, change management and termination, and enforcement of related remote working and password control policies. Access to the application and Customer Data are controlled by use of login/password mechanisms as applicable to the Service purchased by Customer.

8.6. Data Security. Revvity has adopted generally recognized industry standard practices to secure Customer Data in transit and at rest.

8.7. Monitoring. Revvity has adopted generally accepted industry practices to monitor security, confidentiality, availability, and performance of the Service. Revvity implements appropriate audit logging and event monitoring capabilities, including protection of systems audit tools, network security, and monitoring systems use. Audit logs are retained in a manner designed to prevent unauthorized access, use, alteration, or destruction.

8.8. Customer Data Management and Return. The Service enables Customer to retrieve and delete Customer Data. Depending on the purchased Service, Customer may not have access to the Service or Customer Data during a suspension of Services or following the expiration or termination of the Service subscription term. Except as otherwise set forth in the SaaS Agreement, Customer is responsible for retrieving a copy of its Customer Data prior to the expiration or termination of the Service, and Revvity may delete Customer Data following the expiration or termination of the subscription term in accordance with the terms of the SaaS Agreement. The Customer Data retrieval capabilities described herein are not back-up capabilities and are not intended to restore Customer's Service to its state at a prior point in time. Disaster recovery and back-up capabilities are described in more detail below.

9. SECURITY INCIDENTS.

9.1. Notification of a Security Incidents. In the event of a Security Incident, Revvity will notify Customer without undue delay after becoming aware of the Security Incident, but in no event later than any periods required by applicable Data Protection Laws or described in the SaaS Agreement. Revvity shall, as part of the notification provided under this Section 9.1 and to the extent reasonably available at the time of notice, provide all information required under applicable Data Protection Laws. Revvity shall update Customer as additional relevant information set forth in the foregoing sentence becomes available without further undue delay. Revvity shall be under no obligation to notify Customer of routine security alerts in respect of the Service (including, without limitation, pings and other broadcast attacks on firewalls or other devices).



9.2. Maintaining Security Incident Documentation. Revvity shall maintain and preserve applicable documents, records, and other data reasonably related to any Security Incident.

9.3. No Admission of Fault. Notwithstanding anything to the contrary, in no event will any notice of a Security Incident under this Section 9 be construed as an acknowledgement of Revvity of any fault or liability of Revvity with respect to any Security Incident.

10. SUBPROCESSORS.

10.1. Use of Subprocessors. Revvity may use Subprocessors to perform the Processing pursuant to this Security and Privacy Addendum. The name and details of the processing to be performed will be amended by Revvity from time to time subject to the terms of this Section 10.

10.2. Subprocessors. To the extent permitted under applicable Data Protection Laws and subject to Revvity's compliance with the remainder of this Section 10, Customer hereby provides a general authorization for Revvity to engage Subprocessors to Process Personal Data in connection with the provision of the Service.

10.3. New or Changed Subprocessors. Revvity shall provide reasonable notification to Customer where Revvity wishes to engage a new Subprocessor to Process Personal Data. Customer shall have thirty (30) days after issuance of such notice to notify Revvity in writing of any objections on reasonable grounds.

10.4. Subprocessor Requirements. Revvity shall ensure that all Subprocessors so engaged are bound by written agreements with terms and conditions at least as restrictive as the relevant terms and conditions contained in this Security and Privacy Addendum. Revvity shall remain fully liable to the Customer for a Subprocessors failure to fulfil its obligations under such agreement.

11. RIGHTS OF THOSE AFFECTED BY PROCESSING. The applicable Data Subjects are the intended third-party beneficiaries of this Security and Privacy Addendum. In this regard, Data Subjects shall be entitled to exercise all rights available to Customer under this Security and Privacy Addendum, and enforce all terms and conditions of this Security and Privacy Addendum to the extent such rights, terms, and conditions impact or otherwise relate to the Processing of such Data Subjects' Personal Data. Each Party shall use reasonable efforts to support the other affected Party in their efforts to safeguard these rights.

12. COMPELLED DISCLOSURES. Any disclosure by Revvity or its representatives of any of the Personal Data pursuant to applicable federal, state, or local law, regulation, or valid order issued by a court or governmental agency of competent jurisdiction (a "**Legal Order**") will be subject to the terms of this Section 12. Prior to making such a disclosure, Revvity shall, to the extent permitted under the Legal Order, make commercially reasonable efforts to provide Customer with: (a) prompt written notice of the disclosure requirements set forth in the Legal Order so that Customer may seek, at its sole cost and expense, a protective order or other remedy; and (b) reasonable assistance, at Customer's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If, after providing such notice and assistance as required herein, Revvity remains subject to a Legal Order to disclose any Personal Data, Revvity shall, upon Customer's request, use commercially reasonable efforts to obtain assurances from the applicable court or agency that such Personal Data will be Processed solely to the extent necessary and otherwise remain confidential.

13. CROSS-BORDER TRANSFERS OF PERSONAL DATA.

13.1. Prohibited Transfers. Neither Customer nor Revvity shall transfer any Personal Data to another country unless the transfer complies with the Data Protection Laws.



13.2. Permitted Countries for Processing; Cross-Border Data Transfer Restrictions. Appendix B lists all of the countries Revvity may receive, access, transfer, or store Personal Data. Revvity must not Process (including through Subprocessors) the Personal Data outside the countries listed on Appendix B without Customer's prior written consent. If applicable Data Protection Laws restricts cross-border Personal Data transfers from certain countries (each such country, an "**Export Restricted Country**"), each Party shall only transfer that Personal Data to the other Party, a Party's Affiliate, or a Subprocessor under the following conditions, as applicable: (a) the recipient of the Personal Data (the "**Data Importer**"), either through its location or participation in a valid cross-border transfer mechanism under the Data Protection Laws, as identified in Appendix B, may legally receive that Personal Data; (b) the transferor of the Personal Data (the "**Data Exporter**") obtained valid Data Subject consent to the transfer, to the extent necessary or permitted under the Data Protection Laws; or (c) the transfer otherwise complies with or is otherwise permitted under the Data Protection Laws.

13.3. Essential Equivalence. The Parties shall assess, taking into account the circumstances of the transfer, whether the level of protection for Personal Data afforded by the Applicable Laws that are applicable to the Data Importer are essentially equivalent to that provided under the Data Protection Laws applicable to the Data Exporter. In the event either Party believes, in its reasonable discretion, that it is unable to comply with the requirements under the applicable cross-border transfer mechanism specified in Appendix B (and any regulations promulgated thereunder, each as amended, supplemented or otherwise modified from time to time in accordance with Applicable Law) or provide such a level of protection to Personal Data, such Party shall notify the other Party of such determination and the Customer may, if it agrees with such determination and the Parties cannot reasonably supplement the cross-border transfer mechanism described in Appendix B with additional terms and conditions that would provide the required level of protection or adopt another cross-border data transfer mechanism that will provide the required level of protection, suspend any further transfers of Personal Data or terminate the SaaS Agreement.

13.4. Standard Contractual Clauses. If any Personal Data transfer between Revvity and Customer requires or otherwise utilizes the execution of the applicable Standard Contractual Clauses in order to comply with the applicable Data Protection Laws, the Parties hereby execute such Standard Contractual Clauses and take all other actions required to legitimize the transfer, including, as necessary: (a) formally executing the applicable Standard Contractual Clauses with a written or electronic signature, as necessary; (b) cooperating to register the Standard Contractual Clauses with any supervisory authority in any applicable country; (c) procuring approval from any such supervisory authority; and (d) providing additional information about the transfer to such supervisory authority.

14. TERM AND TERMINATION.

14.1. Term. The term of this Security and Privacy Addendum will commence on the Effective Date and will remain in force until the earliest date that: (a) this Security and Privacy Addendum is replaced or repealed by mutual agreement of Customer and Revvity; (b) this Security and Privacy Addendum is replaced by an alternative agreement in order to meet additional or changed rights and obligations under Data Protection Laws; or (c) the SaaS Agreement is terminated or expires (the "**Term**").

14.2. Survival. In the event Revvity retains Personal Data after the Term for any reason, Revvity shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Personal Data, and such obligations shall survive past the Term of this Security and Privacy Addendum until such time that Processor and all of its Subprocessors no longer Process such Personal Data. In addition, any provision of this Security and Privacy Addendum that expressly or by implication should come into or continue in force on or after such period described in the foregoing sentence in order to protect Personal Data will remain in full force and effect.



14.3. Changes in Data Protection Laws. If a change in any of the Data Protection Laws prevents either Party from fulfilling all or part of its obligations under the SaaS Agreement or this Security and Privacy Addendum, the Parties shall negotiate a change to this Security and Privacy Addendum, the Services, or the SaaS Agreement in good faith and shall suspend the Processing of Personal Data until that Processing complies with the new requirements. If the Parties are unable to bring the Processing of Personal Data into compliance with the Data Protection Laws within a reasonable period, they may terminate the SaaS Agreement upon written notice to the other Party.

15. PERSONAL DATA RETURN AND DESTRUCTION.

15.1. Return or Destroy Personal Data. The Services include certain features that allow Customer to delete or obtain a copy of all Personal Information Processed by Revvity for Customer. Upon a reasonable time after the termination or expiration of this Security and Privacy Addendum for any reason as set forth in the SaaS Agreement: (a) Revvity shall, and shall require all Subprocessors to, cease Processing Personal Data except as otherwise set forth hereunder; and (b) Revvity shall, and shall require all Subprocessors to, securely destroy all or any Personal Data related to this agreement in its possession or control.

15.2. Retention of Data on Backup; Retention Required by Law. Notwithstanding the foregoing, to the extent it is not commercially reasonable for Revvity or its Subprocessors to remove Personal Data from archive or other backup media, Revvity may retain Personal Data on such media in accordance with its backup or other disaster recovery procedures. If any Applicable Law or Legal Order requires Revvity to retain any Personal Data that Revvity would otherwise be required to return or destroy, it shall notify Customer in writing of that retention requirement, giving details of the Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

16. MISCELLANEOUS.

16.1. Amendment. This Security and Privacy Addendum may not be amended or modified except in writing signed by authorized representatives of both Parties.

16.2. Severability. If any provision in this Security and Privacy Addendum is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the Security and Privacy Addendum and the SaaS Agreement shall not be affected. The Parties shall promptly and in good faith replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly promptly and in good faith add any necessary appropriate provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this Security and Privacy Addendum is subject.

16.3. Governing Law. This Security and Privacy Addendum shall be governed by and construed in accordance with law that governs the SaaS Agreement.

16.4. Headings. The headings in this Security and Privacy Addendum are for reference only and shall not affect the interpretation of this Security and Privacy Addendum.



Appendix A

Data Processing Purposes and Details

1. **Nature of the Processing.** Data storage and such other Services as initiated by Customer from time to time.
2. **Purposes of the Processing.** The purpose of the data processing under this Security and Privacy Addendum is the provision of data storage and such other Services initiated by Customer from time to time.
3. **Categories of Data Subjects.** The data subjects may include Customer's customers, employees, vendors, and end users.
4. **Categories of Personal Data.** Categories of personal data include any personal data uploaded by Customer.
5. **Sensitive Data Processed (if any).** The data processed is determined by customer. Sensitive data will be processed if uploaded by Customer. Only the categories of sensitive data uploaded by customer will be processed.
6. **Duration of Processing.** The duration of the processing is determined by the Customer.
7. **Frequency of Processing.** Data will continue to be stored until deleted by customer or deleted as a result of account termination.



Appendix B
Countries of Processing and Legal Basis for Transfers

REVVITY HEALTH SCIENCES, INC. SUBPROCESSOR INFORMATION

1. **REVVITY AFFILIATES.** Revvity Health Sciences, Inc. may engage certain of its affiliates (as listed in its most recent 10-K filing, and as otherwise may be added from time to time) to act as subprocessors to provide services relating to the operation of its software-as-a-service ("**SaaS**") solutions (including cloud monitoring and security), to provide maintenance or technical support services, or to provide professional services.
2. **SOFTWARE AS A SERVICE.** The following subprocessors might be used in the provision of Revvity's cloud offerings as more specifically set forth below:

Name	Location	Purpose
Amazon Web Services	As set forth in Revvity's Quotation	Cloud provider
AT&T AlienVault	U.S.A.	Security monitoring, threat detection & logging
DataDog	As set forth in Revvity's Quotation	Logging, tracing and alerting
Qualys	U.S.A.	Vulnerability detection and Web Application Scanning
Checkmarx	U.S.A.	Static code Analysis
PagerDuty	U.S.A.	Incident Response Management
Auth0	As set forth in Revvity's Quotation	Authorization and authentication

3. **PROFESSIONAL SERVICES/TECHNICAL SUPPORT.** These following subprocessors may be utilized to provide professional services and/or technical support to customers. Customer is always in control of what personal data is shared when engaging Revvity, and its applicable subprocessors, for professional services and support.

Name	Location
SII	Poland
SailsSoftware	India



ANNEX: TECHNICAL SUPPORT TERMS AND CONDITIONS

1. Applicability. The terms and conditions of this Annex applies to Revvity™ Genomics LIMS, Revvity™ Genomics Analyze, Revvity™ Genomics Interpret, EVOYA, and Transcribe AI. A separate annex governs technical support for OZ SaaS software.

2. Technical Support. The Customer shall communicate all Technical Support issues by phone or e-mail. “**Technical Support**” includes (i) Diagnosis of problems or issues with the Service; (ii) Reasonable commercial efforts to resolve reported and verifiable errors in the Service so that the Service performs in all material respects as described in the Documentation; (iii) Technical and Non-technical Customer service assistance during normal Revvity business hours. For U.S.: 08:00 AM to 05:00 PM. For EMEA: 09:00 AM to 05:00 PM EET.

3. Priority Level Definitions & Response Times. All Technical Support requests must be directed to Revvity’s Technical Support team. All Technical Support cases are assigned to a specialist and prioritized based on the severity and visibility of the issue. Technical Support will attempt to troubleshoot the issue and provide a workaround solution, or it will file a defect in Revvity’s defect tracking system for remediation. Revvity will use commercially reasonable efforts to respond to requests and problems that reflect the urgency of the resolution of a request. A “resolution” can be any of the following: a work around, hotfix, service release, or an action plan to address the issue.

Priority Level	Definition	Initial Response Target	Target Resolution Method
Urgent	• System does not allow the Customer to view or enter result or case data necessary to determine if a sample indicates risk for a disorder • System produces results that are not equivalent to those expected to be produced as defined in the agreed upon specifications and the results cannot be modified prior to being reported • System cannot perform a function that is required for results to be reported within the lab’s standard turn-around time for a single specimen • System presents an error that prevents the completion of a reporting task and the task cannot be completed by a reasonable workaround • System cannot be accessed	4h	Hotfix or workaround
Moderate	• System presents an error. However, results can be reported within the lab’s standard turn-around time for a single sample and actions can be performed within the follow-up system by using a reasonable workaround. • System performance is delayed. However, results can be reported within the standard lab turn-around time for a single sample and actions can still be performed within the follow up system by using a reasonable workaround. • System does not allow an individual access to a specific module.	1d	Service release or workaround
Minor	• An error in visual presentation, including misspelling or incorrect order or display of columns.	3d	Major release or workaround

4. Initial Priority Level. At the time Revvity accepts a Technical Support request, Revvity will record an initial Priority Level based on the above Priority Level definitions. Upon acceptance of a Technical Support request, Revvity’s initial focus will be to resolve the issues underlying the request. The Priority Level of the request may be adjusted as described below.

5. Downgrade or Upgrade of Technical Support Request Priority Levels. If, during the Technical Support request process, Revvity determines the issue no longer warrants the Priority Level currently assigned or warrants the assignment of a higher priority level than currently assigned, based on its current impact on the operation of the Service, then the Priority Level will be downgraded or upgraded by Revvity to the priority level that most appropriately reflects its current impact.

6. Resolution Times. Due to the widely varying nature of possible issues, it is not possible to provide specific resolution objectives. Revvity will use commercially reasonable efforts to resolve all reported and verifiable issues with the Service as promptly as possible and in accordance with the Priority Levels assigned to such issue.



CLOUD SERVICE SECURITY ADDENDUM

(Cloud Service Security Description - CSSD)

Revvity operates SaaS cloud services for its customers under a documented quality and information security management system and provides the Cloud Service (defined in Section 1) to the Customer pursuant to a master services agreement, subscription agreement or equivalent contract between Revvity and the Customer (the "**Main Agreement**").

This Cloud Service Security Addendum (the "**Addendum**") describes the security capabilities, shared responsibilities, and compliance posture applicable to the Cloud Service, in accordance with ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, and supplements the Main Agreement.

1. DEFINITIONS. Capitalized terms used but not defined in this Addendum have the meanings given to them in the Main Agreement. For the purposes of this Addendum:

- i. "**Cloud Service**" means the cloud-based service(s) made available by Revvity to the Customer under the Main Agreement.
- ii. "**Customer Data**" means data uploaded to or generated within the Cloud Service by or on behalf of the Customer, including Personal Data.
- iii. "**CSSD**" means this Cloud Service Security Description, as updated from time to time.
- iv. "**ISMS**" means Revvity's Information Security Management System.
- v. "**PII**" means personally identifiable information, including Personal Data as defined under Regulation (EU) 2016/679 (GDPR).
- vi. "**PII Controller**" and "**PII Processor**" have the meanings given in ISO/IEC 29100 and, where applicable, in GDPR.
- vii. "**RTO**" means Recovery Time Objective; "**RPO**" means Recovery Point Objective.

2. SECURITY GOVERNANCE AND COMPLIANCE

2.1 Management System. Revvity operates an ISMS aligned with ISO/IEC 27001. Cloud-specific controls are aligned to ISO/IEC 27017 (cloud security), and the protection of personally identifiable information is aligned to ISO/IEC 27018.

2.2 Underlying Cloud Providers. The Cloud Service is hosted with third-party cloud service providers that are required to hold ISO/IEC 27001 certification or, as a minimum, a SOC 2 Type 2 attestation. Physical and environmental controls at the hosting facilities are inherited from such providers.

2.3 Certifications and Evidence. Revvity shall make available to the Customer, on reasonable request and under appropriate confidentiality obligations, copies of its then-current certifications and summary independent audit reports applicable to the Cloud Service.

2.4 Regulatory Compliance. Revvity shall operate the Cloud Service in compliance with applicable data-protection laws, including GDPR where applicable, and supports its customers in meeting their own regulatory obligations (including, where relevant, HIPAA for Protected Health Information).

2.5 Penetration Testing. Revvity contracts with an independent third party to conduct an annual penetration test of the cloud platform, covering network, system and application layers.

2.6 Governing Framework. The legal jurisdiction(s) governing the Cloud Service are those specified in the Main Agreement.

3. SHARED RESPONSIBILITY MODEL

3.1 Principle. Security of the Cloud Service is organized around a shared responsibility model distinguishing "security of the cloud" (infrastructure, hardware, networking and facilities, provided by the underlying cloud provider) from "security in the cloud" (configuration, data, access, operated by Revvity and the Customer).

3.2 Allocation. The allocation of responsibilities between Revvity and the Customer is summarized in the table below. This table is indicative; the Main Agreement prevails in case of conflict.



Security Domain	Revvity Responsibility	Customer Responsibility
Physical security	Inherited from ISO 27001-certified cloud providers	None
Network security	VPC/network segmentation, WAF, IDS/IPS, security groups, TLS 1.2+	Customer-side network and endpoint security
Infrastructure patching	Guest OS, middleware and platform patching per internal patching process	None
OS hardening	CIS benchmark-based hardening, automated drift detection	None
Application security	Secure SDLC, code review, SAST/DAST, annual penetration test	Acceptable use per Main Agreement
Encryption at rest	FIPS 140-2 aligned (AES-256) via managed key service	None
Encryption in transit	TLS 1.2+, HTTPS and SFTP/FTPS for external interfaces	Use of compatible clients and protocols
Identity & access management	IAM, MFA and SSO (SAML/OIDC) capabilities	Manage users, roles and credentials
User provisioning	Provide provisioning functions; semi-annual access review	Timely provisioning and deprovisioning of Customer users
Data classification	Framework (Public/General/Proprietary/Confidential) and tooling	Classify data per Customer policy
Backup & recovery	Daily backups, air-gapped copies, annual DR testing	Request restores, verify data
Incident management	Detection, response, notification (SEV 1/2/3, PII breach)	Report events, manage Customer-side response
Logging & monitoring	24x7 SOC, SIEM, application, API and security event logs	Review available logs, define Customer-side alerts
Vulnerability management	Continuous scanning, SAST daily, DAST weekly, SLA-driven remediation	Report Customer-discovered vulnerabilities
Business continuity	DR plan with RTO 48h / RPO 24h (adjustable per contract)	None
Compliance & audit	Provide certifications and audit evidence on request	Customer-specific regulatory compliance
Data disposal	NIST 800-88 Rev.1 aligned secure deletion at contract end	Export data before termination, confirm destruction

4. GEOGRAPHIC LOCATIONS

4.1 PII Location Register. Revvity maintains a PII Location Register for each cloud product, identifying the primary cloud region(s) and availability zones, the backup/DR region(s), and the locations of any sub-processors. The PII Location Register is made available to the Customer on request.

4.2 Processing and Personnel Access. Customer Data is processed in the hosting region(s) identified in the service description or order form. Revvity personnel authorized to access Customer Data operate from locations disclosed to the Customer on request.

4.3 Location Changes. Revvity shall notify the Customer in writing at least thirty (30) days before any change to the region(s) in which Customer Data is stored or processed. In the case of an emergency disaster-recovery event, notification shall be provided within forty-eight (48) hours after the event.

4.4 Cross-Border Transfers. Cross-border transfers of PII are carried out only (i) to a jurisdiction recognized as providing adequate data protection, (ii) under appropriate safeguards such as Standard Contractual Clauses or Binding Corporate Rules, or (iii) with the Customer's explicit authorization.

5. CRYPTOGRAPHIC CONTROLS



5.1 Data at Rest. Customer Data at rest is encrypted using industry-standard algorithms (AES-256), in alignment with FIPS 140-2 requirements.

5.2 Data in Transit. Customer Data in transit over public networks is protected using TLS 1.2 or higher. Secure file exchange is supported via HTTPS, SFTP and FTPS. TLS 1.2+ is also required for internal inter-network communication.

5.3 Key Management. Cryptographic keys are managed through a managed key service (AWS KMS or equivalent) backed by FIPS 140-2 validated hardware security modules. Keys are used for a single purpose and are protected across their full lifecycle (generation, storage, use, rotation, destruction). A centralized password manager protected by multi-factor authentication is used as the authoritative key/secret vault.

5.4 Rotation. IAM access keys are rotated at least every ninety (90) days and are disabled if inactive for more than ninety (90) days. External TLS certificates are issued by external Certification Authorities with a maximum two (2) year expiry.

5.5 Cryptographic Erasure. At service termination or storage reallocation, cryptographic erasure (deletion of the applicable KMS key) is used as the preferred sanitization method; secure overwrite or physical destruction, in line with NIST 800-88 Rev.1, is used where cryptographic erasure is not applicable.

6. BACKUP, RESTORATION AND BUSINESS CONTINUITY

6.1 Recovery Objectives. Unless otherwise agreed in the Main Agreement, the default recovery objectives for the Cloud Service are Recovery Time Objective (RTO) of forty-eight (48) hours and Recovery Point Objective (RPO) of twenty-four (24) hours. These values may be adjusted on a case-by-case basis to meet specific Customer requirements.

6.2 Backup Scope and Schedule. Backups cover customer databases, customer file uploads, configuration data, system configurations and infrastructure. Backups are performed on a regular schedule (typically daily incremental with periodic full backups).

6.3 Backup Methods and Protection. Backups are performed using cloud-native mechanisms (e.g. managed database snapshots, block-storage snapshots, object-storage versioning). Backup data is encrypted at rest (AES-256) and in transit (TLS 1.2+).

6.4 Storage Locations. Primary backups are stored in the same region as production (separate availability zone); disaster-recovery backups are stored in a geographically separated secondary region; air-gapped daily copies are stored in immutable archive storage to protect against ransomware and destructive events.

6.5 Integrity and Testing. Backup integrity is verified using cloud-native validation features. Disaster-recovery and restoration procedures are tested at least annually.

6.6 Restoration Requests. The Customer may submit restoration requests through the support channel, specifying the data, the backup date and the reason. Planned restorations require Customer authorization; emergency disaster-recovery restorations may be authorized by Revvity. Restoration activities are logged and retained for three (3) years.

6.7 Service Interruption Communications. On declaration of a failover, Revvity shall notify the Customer contract contact by email with the "Unplanned Outage" notice and shall issue an "Availability Restored" notice once service is resumed.

7. ACCESS CONTROL AND AUTHENTICATION

7.1 Principle of Least Privilege. Access to systems containing Customer Data is granted on a need-to-know basis following the principle of least privilege. Shared, generic or group accounts are prohibited for systems containing Customer PII.

7.2 User Lifecycle. Account creation, modification and deactivation follow a documented workflow with manager and Revvity approval. Accounts inactive for ninety (90) days are disabled and, where technically feasible, deleted thirty (30) days after being disabled.



7.3 Access Review. Reviews of access to in-scope systems are performed at least semi-annually. Monthly termination testing is performed for tools not federated with single sign-on or Active Directory.

7.4 Multi-Factor Authentication and Federation. Multi-factor authentication is supported and is required for privileged and administrative accounts. Integration with third-party identity providers (SAML, OIDC) is supported. Passwords used by Revvity personnel meet a minimum complexity policy (at least 8 characters, mixed case, with numbers) and are distributed only through secure channels to verified recipients.

7.5 PII Authorized Users Register. Revvity maintains a register of personnel with access to Customer PII. A Customer-specific, redacted extract of this register is made available to the Customer upon validated request, through secure delivery, within ten (10) business days.

7.6 Temporary Access for Support. Direct Revvity access to production Customer PII is permitted only where (i) a documented support case with business justification exists, (ii) the Customer has provided explicit written authorization, and (iii) Revvity has approved. Such access is time-limited, read-only unless otherwise approved, and fully logged.

8. INCIDENT MANAGEMENT

8.1 Incident Response Process. Revvity operates a documented cyber security incident response process, coordinated through a dedicated incident response team under the authority of Revvity's Legal Department and CISO.

8.2 Severity Levels. Incidents are classified as SEV 1 (Blocker), SEV 2 (Major) or SEV 3 (Minor) based on impact to confidentiality, integrity, availability or Customer operations.

8.3 Customer Notification. Customer-facing incident notifications for SEV 1 and SEV 2 incidents are reviewed and approved by Revvity's Legal Department before delivery. Notification timelines and methods are summarized below.

Severity	Scope	Delivery	Timeframe
SEV 1 - Blocker	Unauthorized access to Customer Data, confirmed data breach or exposure, service disruption exceeding 2 hours, ransomware or destructive malware, compromise of Customer credentials	Phone call to the Customer security contact, followed by email	Immediate (email within 1 hour after legal approval)
SEV 2 - Major	Suspected unauthorized access under investigation, DDoS affecting service, security control failure, sophisticated failed intrusion attempts	Email to the Customer security contact	Within 5 business days
SEV 3 - Minor	Minor issues without direct Customer impact	Logged internally; disclosed on request	As applicable

8.4 PII Breach Notification. Where an incident is confirmed to involve a breach of Customer PII, Revvity shall notify the affected PII Controller within seventy-two (72) hours of confirmation. The notification shall include the nature of the breach, categories and approximate number of PII principals affected, likely consequences, and the measures taken or proposed. An investigation update shall follow within seven (7) days and a final incident report within thirty (30) days.

8.5 Delayed or Waived Notification. Notification may be delayed only where required by law enforcement, ongoing investigation confidentiality or technical complexity, in each case with documented justification and Legal Department approval. Notification may be waived where the affected PII was encrypted with keys that were not compromised and the residual risk to PII principals is negligible; such waiver requires joint approval by Revvity and its Data Protection Officer.



8.6 Customer Reporting Channel. The Customer may report suspected security incidents to Revvity by email to digitalproducts.cloudsecurity@revvity.com, through Contact support email, or through its designated Product Owner or Software Services contact. Ticket status is visible through the support system.

8.7 Digital Evidence and Legal Hold. Upon authorized request, Revvity can provide application and infrastructure logs, snapshots, and other digital evidence, with chain-of-custody controls (SHA-256 hashing, encrypted transfer, recorded handling). Legal hold notices are acknowledged within one (1) business day and maintained until released by Legal Counsel.

8.8 Records Retention. PII breach notification records and incident files are retained for a minimum of seven (7) years.

9. CHANGE MANAGEMENT COMMUNICATIONS

9.1 Change Categories and Notification Timelines. Changes are categorized as Standard, Non-Standard or Emergency. Customer notification timelines are as follows (subject to any specific timelines agreed in the Main Agreement):

Change Type	Examples	Customer Notice
Standard	Pre-defined, tested operations (e.g. scheduled capacity changes, routine access changes)	At least 30 calendar days in advance
Non-Standard	Non-scheduled infrastructure changes, hot-fixes, vulnerability remediations, security patching	At least 7 calendar days in advance where Customer impact is expected
Emergency	Actions to restore service after an outage or to remediate a critical security vulnerability	Within 48 hours after, where Customer impact is expected

9.2 Notification Content. Customer notifications include: change summary, business justification, Customer impact analysis, required Customer actions (if any), timeline, rollback plan, and support contact information. Notifications are delivered through Product Owners, account managers or in-product notifications.

9.3 Customer Objection. For Standard changes, the Customer may submit an objection within fifteen (15) days of notification through its account manager or support channel. Revvity will, where feasible, delay the change for that Customer or propose an alternative solution, and will document the resolution.

9.4 Emergency Changes. Emergency changes may be implemented prior to Customer notification where necessary to restore service or to mitigate a critical security risk; justification is documented and retrospective notification is provided.

9.5 PII Protection Impact Assessment. A PII Protection Impact Assessment (PPIA) is conducted before introducing a new cloud service or significantly modifying an existing service that processes PII.

10. SECURE DEVELOPMENT AND VULNERABILITY MANAGEMENT

10.1 Secure SDLC. Revvity applies a secure Software Development Lifecycle covering design, coding, peer review, testing and release, with Infrastructure-as-Code for production changes and mandatory code review (pull-request approval by a second engineer).

10.2 Security Testing. Security testing includes static application security testing (SAST), dynamic application security testing (DAST), and continuous vulnerability scanning. The typical cadence is:

Scan Type	Cadence
Static code analysis	Daily
Web application scan (DAST)	Weekly
Infrastructure vulnerability scan	Continuous
Third-party penetration test	Annual
Other sources (vendor advisories, CVE)	Ad hoc / continuous



10.3 Remediation SLAs. Vulnerabilities identified in production environments are triaged and remediated according to the following target timeframes (actual timeframes may be impacted by third-party dependencies):

Severity	Acknowledgement	Target Remediation
Blocker (Very High)	Within 4 hours	Fix or workaround within 48 hours
Critical (High)	Within 1 business day	Fix or workaround within 15 days
Major	Within 2 business days	Fix within 45 days
Minor	Within 5 business days	Fix in next release
Trivial	Within 10 business days	None required

10.4 Customer Vulnerability Reports. The Customer may report suspected vulnerabilities through the support channel. Reports are acknowledged within two (2) business days and validated within ten (10) business days, after which remediation follows the SLAs above. The reporter is notified upon completion.

10.5 Customer Vulnerability Disclosure. On request, Revvity provides Customer-specific vulnerability status information, prepared by Revvity's security function and reviewed by Revvity's quality function.

10.6 Hardening. Operating systems and key platform components are hardened in accordance with CIS benchmark standards, with automated drift detection against an Infrastructure-as-Code baseline.

11. DATA CLASSIFICATION, LABELLING AND LIFECYCLE

11.1 Classification Framework. Revvity applies a four-tier data classification framework (Public, General, Proprietary, Confidential). Customer application data containing PII/PHI is, by default, classified as Confidential and subject to the highest level of security controls.

11.2 Customer Labelling. Where supported by the Cloud Service, the Customer may classify and label Customer Data in line with its own information classification policy. Revvity shall not unilaterally reclassify Customer Data.

11.3 Retention. Customer application data is retained for the duration of the Main Agreement and, unless otherwise instructed by the Customer, for a three (3) month transfer window following contract expiration. Other records relating to Customer PII are retained in accordance with the retention schedule specified in the applicable PII processing record.

11.4 Disposal, Return or Transfer. At service termination, the Customer may choose return, transfer to another processor, or deletion of Customer PII. Exports may be provided in agreed formats (e.g. SQL dump, CSV, JSON, Parquet). Deletion is performed in line with NIST 800-88 Rev.1, covering production databases, backups, DR copies, log files, test environments and any sub-processor copies. A Certificate of Destruction is issued to the Customer upon completion.

11.5 Sub-Processors. Revvity engages sub-processors only under contractual obligations consistent with this Addendum. Sub-processor locations are disclosed in the PII Location Register.

12. LOGGING, MONITORING AND TRANSPARENCY

12.1 Logging. Systems handling Customer Data or enforcing access-control decisions record audit logs. Logs are aggregated into a SIEM, stored in append-only storage with tamper detection and cryptographic checksums, and retained by default for one (1) year, four (4) months and fifteen (15) days (configurable by Customer need). All system clocks are synchronized (UTC, ± 1 second accuracy).

12.2 Customer-Available Logs. Upon request, the Customer may obtain application audit logs (authentication, account changes, data modifications, configuration and permission changes, exports), API activity logs and security event logs (failed authentication, account lockouts, MFA events, suspicious-IP detections).



12.3 Customer Investigations. Revvity assists the Customer in investigating events, providing correlated log data and analysis within five (5) business days of a validated request.

12.4 Monitoring and Transparency. Security-related events are monitored by a 24x7 Security Operations Center. Where available for the product, a service-availability status page, planned-maintenance notifications and incident status updates are provided. Infrastructure and application 24x7 proactive monitoring is made ensuring 1 hour response time in case the system cannot be accessed.

13. SCALABILITY

Infrastructure scalability is built on the following principles:

- All resources are scalable. Some of the components are automatically scaled by AWS. For the rest, by default, horizontal scaling is used. If the component cannot be easily scaled horizontally, then vertical scaling is used.
- When resources are scaled horizontally, they should be evenly distributed between Availability Zones.
- When possible, automatic scaling should be used with predefined min and max boundaries. Minimum boundary should be, by default, set to 2. Maximum boundary should be flex enough, but still it needs to be set to avoid high costs in a situation where error causes load to increase. Alerts must be used before the maximum is reached to detect scaling issues.
- Load testing (both maximum load and realistic production load) is used to detect bottlenecks and determine reasonable scaling rules and min/desired/max boundaries.
- Maximum load figures (concurrent users/request volumes) and minimum resource provisioning reaction times are available upon customer request

14. TERM, UPDATES AND GENERAL PROVISIONS

14.1 Term. This Addendum enters into force on the Effective Date and remains in force for so long as the Main Agreement remains in force.

14.2 Updates to CSSD. Revvity reviews this Addendum when there are significant changes to the security architecture, certifications or applicable regulatory requirements.

14.3 Relationship to Main Agreement. In the event of any conflict between this Addendum and the Main Agreement, the Main Agreement shall prevail unless expressly stated otherwise.

14.4 No Additional Warranties. Except as expressly set out in the Main Agreement, nothing in this Addendum creates any additional warranty or representation.

14.5 Governing Law. This Addendum is governed by, and shall be construed in accordance with, the governing law specified in the Main Agreement.

14.6 Entire Agreement. This Addendum, together with the Main Agreement, constitutes the entire agreement between the Parties with respect to its subject matter.