Software Subscription Agreement (Hosted)

Version: 2.1

Last Updated: 1st May 2025

PLEASE READ THIS **SOFTWARE SUBSCRIPTION AGREEMENT (HOSTED)** (the "AGREEMENT") CAREFULLY BEFORE USING THE SECLORE PRODUCTS THAT YOU OBTAINED FROM SECLORE OR AN AUTHORIZED RESELLER. THE TERMS AND CONDITIONS OF THIS AGREEMENT GOVERN YOUR USE OF SECLORE PRODUCTS UNLESS YOU AND SECLORE HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING YOUR USE OF THE SECLORE PRODUCTS. **BY CLICKING THE "I ACCEPT" BUTTON, YOU REPRESENT AND WARRANT TO SECLORE THAT YOU ARE AUTHORIZED BY YOUR COMPANY TO ENTER INTO THIS AGREEMENT. BY USING THE SECLORE PRODUCTS, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SECLORE PRODUCTS.**

This Agreement is entered into by and between Seclore and you, on behalf of yourself and your company ("**Customer**"); each a "**Party**" and collectively the "**Parties**."

Now, therefore, in consideration of the mutual covenants and promises contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS

a. **Affiliate** means any corporation or other business entity, now or hereafter existing, that controls, or is controlled by, or is under common control with a Party, and "Control" means ownership, directly or indirectly of fifty percent (50%) or more of the voting interest of the Party.
b. **Authorized Reseller** means any of Seclore's authorized resellers or other business partners.
c. **Business Day** means any day of the week (excluding Saturdays, Sundays, and public holidays) on which commercial banks are open for business in India and United States, UAE, KSA and Germany.
d. **File Data** means the information stored by Seclore as part of the Services, which provides for digital rights management of Files and is limited to: (i) full name of Users and External Users; (ii) e-mail ID of Users and External Users; (iii) user ID of Users and External Users; (iv) Internet Protocol address of Users and External Users, (v) machine details of Users and External Users; (vi) activity date of Users and External Users; (vii) password of External Users; (viii) File ID; and (ix) File Name, File permissions, encryption keys and activity logs of the Users and External users (which documents the Files accessed by a User and/or External User and actions performed by said User and/or External User on each File).
e. **Confidential Information** means all non-public information disclosed by a Party to the other Party which: (i) is marked as "Confidential" or with a comparable legend if disclosed in written, graphic, machine readable or other tangible form, or (ii) is designated "Confidential" or comparable language at the time of disclosure and summarized in writing to the receiving Party within ten (10) calendar days after such disclosure. Confidential Information further includes without limitation, the Services and the terms and conditions of this Agreement. Confidential Information does not include information which: (a) is now generally known or available or which, hereafter through no act or failure to act on the part of recipient, becomes generally known or available; (b) is rightfully known to recipient at the time of receiving such information; (c) is furnished to recipient by a third Party without restriction on disclosure; or (d) is independently developed by recipient without having relied on the Confidential Information of the disclosing Party.
f. **Customer Application** means an online application that Customer (or a third party acting on Customer's behalf) creates and which interoperates with the Services and/or Software (if applicable) through its published Application Programming Interface ("**API**").
g. **Customer Data** means all electronic data or information which is stored in Files that are created by a User and where access to and control of such Files is managed by the Services.
h. **Effective Date** means the date on which Customer accepts the terms of this Agreement.
i. **External User** means an individual with whom a User intends to share Files.

j. **Documentation** means the files integrated into the Software under the "Help" menu delivered as part of the Software download package.
k. **File** means any document, including without limitation e-mail, protected using the Services.
l. **Intellectual Property Rights** means any intellectual property rights, including patents, utility models, rights in designs, copyrights, moral rights, topography rights, database rights, trademarks, service marks, trade secrets, and rights of confidence, in all cases whether or not registered or registerable in any country, and including the right to apply for the same and all rights and forms of protection of a similar nature or having equivalent or similar effect to any of these anywhere in the world from time to time.
m. **Malicious Code** means viruses, worms, time bombs, trojan horses and other harmful or malicious code, files, scripts, agents, or programs.
n. **Order Form** means a Customer document (or, if Customer is purchasing the Services through an Authorised Reseller, such Authorised Reseller's purchase order) which has been accepted by Seclore in writing (which may be via e-mail), and which identifies the Subscription Term, Services and/or Software or, if applicable, NREs (*as defined below*), to be provided hereunder.
o. **Seclore** means (i) Seclore Inc., if Customer has purchased Services in United States; (ii) Seclore Technology Private Limited, if Customer purchased the Services in India; (iii) Seclore Technologies FZ LLC, if Customer purchased Services in United Arab Emirates (UAE) and Kingdom of Saudi Arabia (KSA); and (iv) Seclore GmbH, if Customer has purchased Services in Germany; and (v) Seclore Technology Private Limited, if Customer purchased Services in any other country other than United States, India, UAE or Germany.
p. **Seclore Agent** means the software application used by Users and External Users to protect and share Files, as applicable, and which may be downloaded as a desktop or mobile application from Apple App Store or Google Play Store. Seclore Agent is licensed under the terms of a click-wrap agreement that requires acceptance prior to use.
q. **Services** means the products and services that are ordered by Customer under an Order Form and made available by Seclore online via a customer login link. Services exclude Third Party Applications (as defined in Section 4 (*Third Party Providers*) below).
r. **Software** means certain software programs, in binary-code version, including any updates thereto, that are delivered to Customer hereunder. Each Order Form sets forth the software components that Seclore has licensed to Customer under said Order Form.
s. **Subscription Term** means that period of time during which the Customer may use the Software and receive Standard Support Services as set forth in the applicable Order Form, together with any renewal term for which the Customer pays fees.
t. **Standard Support Services** means Seclore's standard support services and service level agreements ("**SLAs**") for the Services, which are detailed in Appendix A hereto.
u. **User** means one named individual authorized by Customer to use the Services and/or Software (if applicable) for the Subscription Term set out on the applicable Order Form, and who has been given a unique user identification by Customer. Under no circumstance may a User subscription be shared among or used by different individuals. Notwithstanding the foregoing, Customer may transfer a User subscription to another user, provided, that the current User no longer has an on-going need to use the Services.
v. **User Guide** means the online user guide for the Services, as updated from time to time.

2. SERVICES

a. **Provision of Services.** Seclore shall make Services available to Customer pursuant to this Agreement and the applicable Order Form during each Subscription Term. Customer agrees that its purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by Seclore regarding future functionality or features. Appendix A attached hereto, sets forth, *inter alia*, Support Services provided by Seclore in connection with the Services.
b. **User Subscriptions.** Unless otherwise specified in the applicable Order Form, (i) Services are purchased as User subscriptions and may be accessed by no more than the specified number of Users, (ii) additional User subscriptions may be added during the applicable Subscription Term, and (iii) the added User subscriptions shall terminate on the same date as the pre-existing User subscriptions. If during a Subscription Term, it is discovered that the Customer has more Users than Customer has purchased subscriptions for, Customer shall be liable to

immediately pay applicable fees for such additional Users (where it shall be deemed that such unreported Users have had access during the full Subscription Term).

c. **Seclore Responsibilities**.

i. **Support Services.** During the Subscription Term, Seclore shall provide Customer with support services in accordance with the support services plan purchased by Customer, as specified on the applicable Order Form. If the support services plan is not identified on the applicable Order Form, Customer shall receive the Standard Support Services. For the purpose of this Agreement, Standard Support Services means the standard Support Services provided by Seclore and identified in Appendix A, (Summary of Support Services by Plan Type (Service Window)).

ii. **Uptime commitment and Service Credits.**

a. **Uptime Percentage.** Seclore shall use commercially reasonable efforts to maintain an "Uptime Percentage" of at least ninety-nine-point five percent (99.5%). Subject to the exceptions noted below, Uptime Percentage will be calculated by subtracting from one hundred percent (100%), the percentage of one (1)-minute periods during any calendar quarter (i.e., three (3) calendar months) in which the Services are Unavailable. "Unavailable" or "Unavailability" means that in any one (1)-minute period, Customer is unable to access and/or protect Files. The Uptime Percentage shall be measured by Seclore in accordance with standard industry practices.

b. **Exclusions from Uptime Percentage.** Notwithstanding anything to the contrary in this Agreement, or elsewhere, any Unavailability issues resulting from or connected to any of the following events will be excluded from the calculation of Uptime Percentage:

i. any downtime during a planned maintenance window, or resulting from changes to Services requested by Customer,

ii. any unavailability caused by circumstances beyond Seclore's reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labour problems, internet service provider and/or hosting service provider failures or delays, or denial of service attacks,

iii. Customer's acts or omissions including, but not limited to, failure of Customer's internet connectivity, Third Party Applications, or any network that is not owned or managed by Seclore.

c. **Service Credits.** If Seclore does not meet the Uptime Percentage with respect to any particular calendar quarter, then as Customer's sole and exclusive remedy for a breach of Section 2(c)(ii), Seclore will provide to Customer a service credit pursuant to the table below ("**Service Credit**"). Service Credits for each quarter can be claimed against the future payments.

Actual Uptime Percentage	**Service Credit**
<99.5% but ≥99.0%	5% of Quarterly fees*
Below 99.0%	10% of Quarterly fees*

*Quarterly Fees shall mean the annual fees paid by Customer during a Subscription Term, divided by four.

d. **Customer Responsibilities.** Customer shall: (i) be responsible for Users' compliance with this Agreement, (ii) be responsible for the accuracy, quality and legality of Customer Data and of the means by which it acquired Customer Data, (iii) use commercially reasonable efforts to prevent unauthorized access to, or use of, the Services and/or Software (if applicable), and notify Seclore promptly of any such unauthorized access or use, and (iv) use the Services only in accordance with the User Guide (and where applicable, use Software in accordance with the Documentation), applicable laws and government regulations. Customer *shall not:* (a) make the Services and/or Software (if applicable) available to anyone other than Users, (b) sell, resell, lend, rent, lease, distribute or otherwise transfer usage rights in the Services and/or Software (if applicable), (c) use the Services and/or Software (if applicable) to transmit infringing, libellous, or otherwise unlawful or tortious material, or to transmit material in violation of third party privacy rights, (d) use the Services and/or Software (if applicable) to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the Services and/or

Software (if applicable), (f) attempt to gain unauthorized access to the Services and/or Software (if applicable) or their related systems or network, or; (g) perform any activities including, but not limited to, reverse engineering, load testing, vulnerability testing, etc., that can potentially disrupt the Services and/or Software (if applicable), without prior written consent from Seclore.

e. **Non-recurring Engineering.** Seclore shall provide one-time, non-recurring (professional) engineering services specified in each statement of work ("**NRE**"). Customer agrees to provide reasonable cooperation for the NRE, including, without limitation, (i) performing the tasks Customer is responsible for performing in a timely manner, (ii) providing Seclore with the information it needs to perform in a timely manner, and (iii) as reasonably needed, providing access to Customer's premises, services, and third party software used in connection with the same. Except for Customer's Confidential Information, Seclore will own all other right, title, and interest in and to all NRE work product and related deliverables, including, without limitation, all Intellectual Property Rights therein. In the event performance of Non-Recurring Services requires travel to Customer's premises, upon mutual prior written agreement, Customer shall reimburse Seclore for reasonable documented travel (i.e., coach class) and related expenses. While on site at Customer's facilities, Seclore will comply with Customer's policies of which Seclore has been made aware in writing.

3. SOFTWARE LICENSE

a. **License Rights.** Subject to the terms and conditions of this Agreement, Seclore grants to Customer during the subscription term, a world-wide, non-exclusive and non-transferable license, without right of sublicense: (i) to permit the number of Users set forth on the applicable Order Form to use Software, if any, as identified on the applicable Order Form, (ii) to copy install and use quantity and type of Software, if any, as identified on the applicable Order Form, and (iii) where Customer has purchased an SDK (Software Development Kit) license, to copy, install and use the SDK solely for purposes of integrating Customer's software application with the Software.

b. **Open Source.** Customer acknowledges that the components of the Services and/or Software may be, provided pursuant to various open-source licenses, and Customer's use of such components shall be governed solely by (and nothing herein shall limit any of Customer's rights under) the applicable open-source licenses. If you wish to obtain a copy of the source code used in the Open-Source Stack and/or the Services and/or Software, please write to support@seclore.com and/or write to attn.: Support Department, Plot No 07 & 08, Excom House, Off Saki Vihar Road, Sakinaka, Andheri (East) Mumbai 400072.

4. THIRD PARTY PROVIDERS

a. **Acquisition of Third Party Products and Services.** From time to time, Seclore utilises several third party products, vendors and libraries and may recommend products or services for Customer ("**Third Party Applications**") to purchase or license from a third party outside of this Agreement ("**Third Party Application Providers**"). Acquisition by Customer of any Third Party Applications, and any exchange of data between Customer and any Third Party Application Provider, is solely between Customer and the applicable Third Party Application Provider. The Customer's use of such Third Party Applications is limited to Customer's own personal, non – transferable and non – exclusive purposes. Customer shall not distribute or resell the Third Party Application to any third party. Seclore does not warrant or support third party products or services, including without limitation, Third Party Applications, whether or not they are designated by Seclore as "approved", 'compatible" or otherwise and such Third Party Applications are provided "as is". Subject to Section 4.c (*Integration with Third Party Applications*) below, no purchase of third party products or services is required to use the Services except a supported computing device, operating system, web browser and Internet connection. Any access to and use of such Third Party Applications is not governed by these terms, but instead shall be governed by the policies of those Third Party Applications. Seclore shall not be responsible for the information practices of such Third Party Applications.

b. **Third Party Applications and Customer Data.** If Customer installs or enables Third Party Applications for use with the Services, Customer acknowledges that Seclore may allow Third Party Application Providers to access Customer Data and File Data, as required for the interoperation and support of such Third Party Applications with the Services. Seclore shall not be responsible for any disclosure, modification or deletion of Customer Data and File Data resulting from any such access by Third Party Application Providers.

c. **Integration with Third Party Applications.** The Services may contain features designed to interoperate with Third Party Applications. To use such features, Customer may be required to obtain access to such Third Party Applications from Third Party Application Providers. If the Third Party Application Providers cease to make the Third Party Application available for interoperation with the corresponding Service features on reasonable terms, Seclore may cease providing such Service features without entitling the Customer to any refund, credit, or other compensation.

5. FEES AND PAYMENT

a. Unless Customer has purchased Services through an Authorized Reseller (in which case Customer shall pay applicable fees to such Authorised Reseller pursuant to a separate agreement between Customer and such Authorized Reseller) Customer hereby acknowledges and agrees as follows:

i. **Fees.** Customer shall pay fees as specified in any Order Form, future Order Forms and as otherwise expressly agreed in writing, signed by both Parties ("**Fees**"). Except as otherwise specified herein; (i) Fees are based on Services purchased and not actual usage; (ii) payment obligations are non-cancellable, and Fees paid are non-refundable; and (iii) the number of User subscriptions purchased cannot be decreased during the relevant Subscription Term stated on the Order Form. Fees are based on annual subscription terms that begin on the subscription start date and renew on each yearly anniversary thereof; therefore, Fees for User subscriptions added in the middle of the Subscription Term will be pro-rated to be co-terminus with the current Subscription Term.

ii. **Annual Uplift.** Effective upon the commencement of any renewal term of a Software subscription, the applicable subscription fees may be increased by an annual uplift; provided, however, that any such increase shall not exceed ten percent (10%) of the subscription fees applicable immediately prior to the renewal term.

iii. **Invoicing and Payment.** Fees will be invoiced in advance. Unless otherwise stated in an Order Form, Fees shall be paid to Seclore: (i) for subscriptions, within thirty (30) days from date of the Order Form and each anniversary of the same, and (b) for NRE, fifty percent (50%) within thirty (30) days from date of the Order Form and fifty percent (50%) upon completion of the same (each a "**Payment Date**"). Customer is responsible for providing complete and accurate billing and contact information to Seclore and notifying Seclore of any changes to such information.

iv. **Overdue Charges.** If any amount or Fees invoiced hereunder are not received by Seclore by the Payment Date, then a service charge of one percent (1.0%) per month or the highest lawful interest rate, whichever is lower, shall be applied to all amounts which are not paid when due under this Agreement, accruing from the Payment Date.

v. **Taxes.** Unless otherwise provided or as required by the applicable jurisdiction, Fees do not include taxes, and Customer is responsible for paying all taxes associated with its purchases hereunder, excluding any taxes based on Seclore's net income or property.

b. **Suspension of Services.** If any Fees under this Agreement, to Seclore or an Authorized Reseller (in the event the Services are purchased via an Authorized Reseller), are thirty (30) days or more overdue, Seclore may, without limiting its other rights and remedies, suspend Services until such amounts are paid in full, provided Seclore has given Customer at least ten (10) days' prior written notice (which may be via e-mail) that its account is overdue. For avoidance of doubt, suspension of Services shall not release Customer of its payment obligations hereunder.

6. PROPRIETARY RIGHTS; AFFILIATES

a. **Reservation of Rights in Services.** Subject to the limited rights expressly granted hereunder, Seclore reserves all rights, title, and interest in and to the Services and/or Software, including all related Intellectual Property Rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

b. **Restrictions.** Customer shall not, directly or indirectly, (i) provide the Services and/or Software (as applicable) on a timesharing, service bureau, hosted, service provider or other similar basis; (ii) remove or alter any copyright, trademark or proprietary notice in or on the Services and/or Software (if applicable); (iii) access or study the Services and/or Software (if applicable) in order to: (a) build a competitive product or services, or (b) copy any features, functions or graphics of the Services and/or Software (if applicable); (iv) modify, translate or create any derivative works based on the Services and/or Software (if applicable); (v) disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that Customer runs (or has run) on the

Services and/or Software (if applicable); (vi) reverse engineer, decompile, disassemble, or otherwise attempt to reconstruct the source code of the Services and/or Software (if applicable); (vii) copy, frame or mirror any part or content of the Services and/or Software (if applicable), other than copying or framing on Customer's own intranets or otherwise for its own internal business purposes.

c. **Ownership of Inventions, Suggestions.** All works of authorship, inventions, discoveries, improvements, methods, processes, formulas, designs, techniques, and information conceived, discovered, developed, or otherwise made by Seclore, solely or in collaboration with Customer, its Affiliates, and/or any third parties relating in any way to the Services and/or Software (if applicable), shall be the sole and exclusive property of Seclore. Customer hereby grants Seclore an irrevocable, royalty-free, unlimited, transferable, worldwide right and license to use, copy, modify, distribute, and make derivative works from any ideas, feedback, suggestions, enhancements, and/or recommendations provided by Customer or its Affiliates relating to the Services and/or Software (if applicable), provided Seclore does not disclose Customer's Confidential Information, or personally identifiable information or Personal Data of Users and that Customer is not identified by Seclore as the provider of any feedback. Any suggestions or feedback are provided "as is" without any warranty.

d. **Affiliates.** Where, in accordance with the terms of the Order Form, Seclore extends Services to Customer's Affiliate(s), the said Affiliate(s) shall have the same usage rights as are granted to Customer, but only during such time as any such entity is an Affiliate of Customer. Customer shall be liable for the acts and omissions of its Affiliates. Any breach of this Agreement by an Affiliate of Customer shall entitle Seclore to terminate this Agreement in accordance with the terms of Section 11(c) (*Termination Rights*) as if Customer were the party in breach. Any termination of this Agreement shall be effective in respect to Customer and all its Affiliates.

7. CONFIDENTIALITY

a. **Obligation.** Seclore and Customer agree that for a period of five (5) years after last receipt of the other Party's Confidential Information, it will: (i) use the other Party's Confidential Information only in connection with fulfilling its rights and obligations under this Agreement; and (ii) hold the other Party's Confidential Information in strict confidence and exercise due care with respect to its handling and protection, consistent with its own policies concerning protection of its own Confidential Information of like importance but in no instance with less than reasonable care, such reasonable care shall include without limitation, ensuring its employees, professional advisors and contractors are legally bound by confidentially obligations that are consistent with the terms and conditions of this Agreement and no less protective of each Party's Intellectual Property Rights as set forth herein, before allowing such parties to have access to the Confidential Information of the other Party.

b. **Exceptions to Obligation.** Notwithstanding Section 7(a) (*Obligation*), either Party may disclose Confidential Information to the extent required by law, provided the other Party uses commercially reasonable efforts to give the Party owning the Confidential Information sufficient notice of such required disclosure to allow the Party owning the Confidential Information reasonable opportunity to object to and to take legal action to prevent such disclosure.

8. WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS

a. **General Warranties.** Each Party warrants that it has the legal power and authority to enter into and perform under this Agreement.

b. **Seclore Warranties.** Seclore warrants for the sole benefit of Customer that: (i) the Services shall be performed materially in accordance with the User Guide; (ii) to the extent Customer has received Software pursuant an Order Form, such Software shall perform materially in accordance with Documentation, (iii) subject to Section 4(c) (*Integration with Third Party Applications*), functionality of the Services will not be materially decreased during a Subscription Term, and (iv) it will not transmit Malicious Code to Customer. Provided however that it is not a breach of this warranty, if Customer or a User uploads a File containing Malicious Code into the Services and later downloads that File containing Malicious Code. For breach of a warranty set forth in Section 8(b), as Customer's exclusive remedy and Seclore's sole liability, Seclore shall correct non-confirming Services and/or Software (if applicable) at no additional charge to Customer, by providing Standard Support Services as set forth in Appendix A. In the event Seclore is unable to correct such deficiencies within one hundred and eighty (180) days by way of providing Standard Support Services, Customer may, as its sole and exclusive remedy for a breach of warranty set forth in Section this 8(b), terminate this Agreement in accordance with Section 11(c) (*Termination*

Rights) and if applicable, obtain refund in accordance with Section 11(d) (*Refund or Payment upon Termination*). To receive the foregoing remedy, Customer must promptly, and in any event no later than five (5) Business days of discovering a breach, provide written notification of such breach to Seclore (a "**Breach Notification**"). Each Breach Notification shall contain a description in sufficient detail to allow Seclore to reproduce the Breach and any further information reasonably requested by Seclore. The warranty set forth in this Section 8(b) shall apply only if (i) Customer is using latest version of the Services, and/or Software(if applicable), and Users and/or External Users are using the latest version of the Seclore Agent; and (ii) the Services have been utilized in accordance with the User Guide (or, in the case of Software, in accordance with the Documentation), this Agreement and applicable law.

c. **Disclaimer.** EXCEPT AS EXPRESSLY SET FORTH IN SECTION 8(b) (*SECLORE WARRANTIES*), SECLORE DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICES WILL BE ERROR-FREE OR RUN FREE FROM INTERRUPTION AND THE SOFTWARE LICENSED HEREUNDER IS LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND. SECLORE MAKES NO OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND AND EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

9. MUTUAL INDEMNIFICATION

a. **Indemnification by Seclore.** In the event of a suit against Customer for use of the Services and/or Software(as applicable), in accordance with the terms and conditions of this Agreement, based upon a claim that the Services and/or Software (if applicable) infringes any valid patent, trademark or copyright, or causes a misappropriation of any trade secret and subject to the limitations set forth in Section 10 (*Limitation of Liability*), Seclore shall defend and indemnify Customer and pay costs and damages finally awarded in any such suit or agreed in any settlement provided that, Seclore is promptly notified in writing of such claim and provided, further that, as a condition precedent to its indemnification obligation Seclore shall have the exclusive right to control such defence or settlement, and Customer shall provide reasonable assistance (at Seclore's expense) in the defence of same. Customer may retain counsel, at its expense, to participate in the defence and settlement of any such claim. In no event shall Customer settle any claim, lawsuit or proceeding or make any admission of liability without Seclore's prior written approval. The foregoing indemnity obligation shall not extend to any claims of infringement arising out of or related to: (i) combination, operation or use of the Services and/or Software (if applicable) with any other products or services not supplied by Seclore including without limit Customer Applications, Third Party Applications, where such combination, operation or use is the cause of such infringement; (ii) modification of the Services and/or Software (if applicable) that was not made by Seclore, or was undertaken at the request of, or direction of, the Customer; (iii) Customer's use of the Services and/or Software (if applicable) in a manner that does not comply with this Agreement, or is not authorized by Seclore; (iv) any claims for damages arising after Seclore's notice to Customer that Customer should cease use of the Services and/or Software (if applicable); or (v) failure of Customer to use upgraded or modified Services and/or Software (if applicable) provided by Seclore to avoid infringement.

b. **Obligation to Correct Services.** Upon notice of an alleged infringement of the Services and/or Software (if applicable) or if in Seclore's reasonable opinion such a claim is likely, Seclore shall, at its sole option, obtain for Customer the right to continue use of the Services and/or Software (if applicable), substitute the Services and/or Software (if applicable) with similar operating capabilities, or modify the Services and/or Software (if applicable) so they are no longer infringing. In the event the foregoing options are not commercially practicable Seclore shall terminate Customer's User subscriptions for such Services and/or Software (if applicable) upon fifteen (15) Business Days' written notice and refund to Customer the unused portion of any prepaid Fees for the Services and/or Software (if applicable) or the affected part thereof.

c. **Indemnification by Customer.** Customer shall defend Seclore against any claim, demand, suit or proceeding made or brought against Seclore by a third party alleging that the Customer Data, or Customer's use of the Services and/or Software (if applicable) in breach of this Agreement, infringes or misappropriates the Intellectual Property Rights of a third party or violates applicable law (a "**Claim Against Seclore**"), and shall indemnify Seclore for any damages, attorney's fees and costs finally awarded against Seclore as a result of, or for any amounts paid by Seclore under a court-approved settlement of, a Claim Against Seclore; provided that Seclore: (a) promptly gives to the Customer written notice of the Claim Against Seclore, (b) gives Customer sole control of the defence

and settlement of the Claim Against Seclore, and (c) provides to Customer all reasonable assistance, at Customer's expense.

d. **Exclusive Remedy.** This Section 9 (*Mutual Indemnification*) states the indemnifying Party's sole liability to, and the indemnified Party's exclusive remedy against, the other Party for any type of claim described in this Section.

10. LIMITATION OF LIABILITY

a. **Limitation on All Damages.** IN NO EVENT SHALL SECLORE'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED IN THE AGGREGATE THE FEES PAID FOR USE OF THE SERVICES IN THE TWELVE (12) MONTH PERIOD PRIOR TO THE EVENT GIVING RISE TO THE DISPUTE.

b. **Disclaimer of Consequential Damages.** IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ANY LOST PROFITS, REVENUE, OR DATA, INTERRUPTION OF BUSINESS OR FOR ANY INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR INDIRECT DAMAGES OF ANY KIND, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN. THE FOREGOING SHALL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS FOR THE SERVICES AND/OR SOFTWARE (IF APPLICABLE).

11. TERM AND TERMINATION

a. **Term of Agreement.** This Agreement commences on the Effective Date and continues in force until terminated in accordance with this Section 11.

b. **Term of User Subscriptions.** User subscriptions commence on the start date specified in the applicable Order Form and unless otherwise specified therein, shall continue for a period of one (1) year. If the start date is not identified in applicable Order Form, User's Subscription Term shall be one (1) year, commencing on the applicable Order Form date. Except as otherwise specified in the applicable Order Form, all User subscriptions shall automatically renew for additional periods equal to the expiring subscription term or one (1) year (whichever is shorter), unless either Party gives the other notice of non-renewal at least thirty (30) Business Days before the end of the relevant Subscription Term. The expiration or termination for any reason of any individual Order Form shall not result in a termination of this Agreement but shall result only in termination of the applicable Order Form. The provisions of this Agreement relating to the effects of termination shall apply to each Order Form as an independent contract.

c. **Termination Rights.** If either Party is in default of any material provision of this Agreement and such default is not corrected within thirty (30) days of receipt of written notice, the other Party shall have the right to terminate this Agreement by providing written notice to the Party in breach. Either Party shall have the right to immediately terminate this Agreement in writing if the other Party: (a) voluntarily or involuntarily becomes the subject of a petition in bankruptcy or of any proceeding relating to insolvency, receivership, liquidation, or composition for the benefit of creditors which is not dismissed within one hundred and twenty (120) days; or (b) admits in writing its inability to pay its debts as they become due.

d. **Refund or Payment upon Termination.** Upon any termination by Customer pursuant to Section 11(c) (*Termination Rights*), Seclore shall refund to Customer the unused portion of any pre-paid Fees covering the remainder of the Subscription Term of all Order Forms after the effective date of termination. Upon any termination for cause by Seclore, Customer shall pay any unpaid Fees covering the remainder of the Subscription Term of all Order Forms after the effective date of termination. In no event shall any termination relieve Customer of the obligation to pay any Fees payable to Seclore for the period prior to the effective date of termination.

e. **Effect of termination; Surviving Provisions.** Customer shall take appropriate steps to un-protect Files prior to termination of the Subscription Term as the Services will not function thereafter. Upon termination of the Agreement as a whole or upon the written request of a Party, each Party shall, at the disclosing Party's option, immediately return or destroy the other Party's Confidential Information received hereunder in its possession or under its control. Customer's obligation to make payment of any unpaid fees and the terms of Sections 5 (*Fees and Payment*), 6 (*Proprietary Rights; Affiliates*), 7 (*Confidentiality*), 9 (*Mutual Indemnification*), 10 (*Limitation of Liability*), 11(d) (*Refund or Payment upon Termination*), 11(e) (*Effect of termination; Surviving Provisions*), 12 (*Data Protection*) and 13 (*General Provisions*) shall survive any termination or expiration of this Agreement.

12. DATA PROTECTION

In the event and to the extent that Seclore Processes (*as defined in Appendix B*) certain Personal Data (*as defined in Appendix B*) on behalf of the Customer, Seclore will comply with the terms and conditions of the Appendix B (Controller-Processor Data Processing Addendum) attached hereto and incorporated herein. The provisions contained in Appendix B, are Customer's complete instructions to Seclore, for the Processing of Personal Data.

13. **GENERAL PROVISIONS**

a. **Notice to Customers based in the United States.**

i. **U.S. Export Compliance.** If the Customer has purchased Services and/or Software (if applicable), in United States, Customer acknowledges that the Services and/or Software (if applicable), are subject to U.S. export control laws, including U.S. Export Administration Act and its associated regulations. Customer agrees to comply with all laws and regulations of the United States to assure that neither the Services and/or Software (if applicable), nor any direct products thereof are: (A) exported directly or indirectly, in violation of such laws, either to any countries that are subject to U.S. export restrictions or to any User and / or External User who has been prohibited from participating in the U.S. export transactions by any federal agency of the U.S. Government; or (B) intended to be used for any purpose prohibited by U.S. export laws, including, without limitation, nuclear, chemical, or biological weapons proliferation. Each Party represents that it is not named on any U.S. government denied party list. Customer shall not permit Users to access or use Services and/or Software (if applicable), in a U.S.-embargoed country (currently Crimea - region of Ukraine) Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation.

ii. **Federal Government End Use Provisions.** If the Customer has purchased Services and/or Software (if applicable) in United States, Customer acknowledges that the Services and/or Software (if applicable), consists of "commercial computer software" and "commercial computer software documentation" as such terms are defined in the Code of Federal Regulations. No government procurement regulations or contract clauses or provisions shall be deemed a part of any transaction between the Parties unless its inclusion is required by law, or mutually agreed in writing by the Parties in connection with a specific transaction. Use, duplication, reproduction, release, modification, disclosure, or transfer of the Services and/or Software (if applicable) is restricted in accordance with the terms of this Agreement.

b. **Publicity.** Within thirty (30) days of the Effective Date and at Seclore's election, the Parties shall issue a joint press release regarding Customer's use of the Services and/or Software (if applicable). In addition, either Party may include the other's name and logo in customer or vendor lists on such Party's website and marketing collateral. Customer also agrees to: (a) serve as a reference or host onsite reference visits; (b) collaborate on press releases announcing or promoting the relationship; and (c) collaborate on case studies or other marketing collateral.

c. **Compliance with Laws.** The Services and/or Software (if applicable) are subject to export control laws. Customer agrees to comply fully with all export and import laws and regulations of the jurisdiction in which it resides ("**Export Laws**") to ensure that neither the Services and/or Software (if applicable), nor any direct products thereof are: (a) exported directly or indirectly, in violation of Export Laws, either to any country that is subject to export restrictions, or to any User and / or External User who has been prohibited from participating in export transactions by any government agency, or (b) intended to be used for any purpose prohibited by Export Laws, including without limitation, nuclear, chemical or biological weapons proliferation.

b. **Relationship of the Parties.** The Parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

d. **Notices.** Any notices required under this Agreement shall be given in writing, shall reference this Agreement, and shall be deemed to have been delivered and given: (a) when delivered personally; (b) three (3) Business Days after having been sent by registered or certified mail, return receipt requested; or (c) one (1) Business Day after deposit with a commercial overnight courier, with written verification of receipt. Notices to Seclore shall be sent to the address listed on the Seclore's website (Seclore's website is currently located at www.seclore.com) and shall be addressed to the "Legal Department". Notices to Customer shall be sent to the address provided in Order Form, and where applicable to the e-mail ID provided by Customer.

e. **Force Majeure.** Except for any payments due hereunder, neither Party shall be responsible for delay or failure in performance caused by any government act, law, regulation, order, or decree, by communication line or power failures beyond its reasonable control, or by pandemics, fire, flood, or other natural disasters or by other causes beyond its reasonable control, nor shall any such delay or failure be considered to be a breach of this Agreement.

f. **Amendment, Waiver.** Seclore reserves the right to modify, update, or change the terms of this Agreement at any time by notifying the Customer through the email address provided by the Customer under this Agreement. The amended Agreement shall become effective immediately upon such notice. The Customer's continued use of the Services and/or the Software (as applicable), after the effective date of any such modifications constitutes it acceptance of the revised Agreement. Upon acceptance of an order by Seclore (which may be by e-mail), the order shall become a non-cancellable Order Form. The Order Form shall constitute an amendment to this Agreement, provided, that the Order Form is in accordance with the terms and conditions of this Agreement. Notwithstanding the foregoing, the only operative terms in an Order Form shall be: (i) the identification of the Services and/or the Software (as applicable), (ii) the Subscription Term, and the number of Users, (iii) the Affiliates that will be using the Services, if any, and (iv) a calculation of the Fees due therefor. A waiver on one occasion shall not be construed as a waiver of any right on any future occasion. No delay or omission by a Party in exercising any of its rights hereunder shall operate as a waiver of such rights.

g. **Data Aggregation.** Customer acknowledges and agrees that the Services and/or the Software (as applicable) transmit anonymous, aggregated data regarding usage to Seclore, solely for audit purposes and improving usage of the Services and/or the Software (if applicable).

h. **Provision Severability**. In the event that it is determined by a court of competent jurisdiction that any provision of this Agreement is invalid, illegal, or otherwise unenforceable, such provision shall be enforced as nearly as possible in accordance with the stated intention of the Parties, while the remainder of this Agreement shall remain in full force and effect and bind the Parties according to its terms. To the extent any provision cannot be enforced in accordance with the stated intentions of the Parties, such terms and conditions shall be deemed not to be a part of this Agreement.

i. **Assignment.** This Agreement is not assignable or delegable by Customer (including, without limitation, by merger, operation of law, or through the transfer of all or substantially all of the equity, assets, or business of Customer), in whole or in part, without the prior written consent of Seclore. This Section shall not be construed as limiting Seclore's right to use subcontractors and its Affiliates to carry out any of its obligations under this Agreement, provided that Seclore shall remain liable for any such Services provided by a subcontractor or Affiliate. Any assignment not in conformity with this Section shall be null and void. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the Parties, their respective successors and permitted assigns.

j. **Governing Law; Jurisdiction**
   i. **United States.** If Customer purchased the Services in United States, California state law governs the interpretation of this Agreement excluding its conflict of laws principles. The state and federal courts located in San Francisco County, California shall have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this Agreement. Each Party hereby consents to the exclusive jurisdiction of such courts.
   ii. **India.** If Customer purchased the Services in India, Indian law governs the interpretation of this Agreement. The courts located in Mumbai, India shall have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this Agreement. Each Party hereby consents to the exclusive jurisdiction of such courts.
   iii. **United Arab Emirates.** If Customer purchased the Services in the United Arab Emirates, laws of the Emirate of Dubai and the federal laws of United Arab Emirates governs the interpretation of this Agreement. The parties hereby submit to the exclusive jurisdiction of the courts of Dubai.
   iv. **Outside United States, India, and United Arab Emirates.** If Customer purchased Services in any other country other than the those listed in (i)-(iii) above, the laws of England and Wales shall apply, without reference to its conflicts of law provisions. Courts located at London shall have exclusive jurisdiction over any dispute arising out of this agreement.
   v. The applicability of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded from this Agreement.

k. **Entire Agreement.** This Agreement, including all appendices and addenda hereto and all Order Forms, constitutes the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter. However, to the extent

of any conflict or inconsistency between the provisions in the body of this Agreement and any appendices or addendum hereto or any Order Form, the terms of such appendices, addendum or Order Form shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

_____End of Page_____

APPENDIX A

SECLORE RIGHTS MANAGEMENT SUPPORT SERVICES AND SLAS

Seclore will provide Support Services in accordance with the following terms and conditions.

A. SCOPE OF SUPPORT SERVICES - The Support Services provided by Seclore will include:

Function	Description
Deployment	Deployment and configuration of the Services in Seclore cloud environment, including role-based access control, cloud virtual network design, and security controls.
Monitoring and upkeep.	Monitoring of the Seclore cloud infrastructure and health of the Services to minimize unplanned interruptions to Services by way of regular internal reviews. Perform capacity planning and review performance metrics of the Seclore cloud environment.
Security	Assess, test, schedule, deploy and manage patching on Seclore cloud environment. Security controls and hardening, antivirus and malware management and monitoring to maintain the health of Seclore cloud environment.
Product upgrade	Periodically upgrade the Services with the latest version. Please refer to the Seclore Product Life Cycle Policy for more information.

B. SUMMARY OF SUPPORT SERVICES BY PLAN TYPE (SERVICE WINDOW)

Support Offerings	Standard	Gold
Upgrades / Bug Fixes (Maintenance Releases)	YES	YES
Web Support through support.seclore.com	* 8 x 5	24 x 7
E-mail Support	* 8 x 5	24 x 7
Phone Support	* 8 x 5	24 x 7
Designated Support Contacts **	2	6
Priority Case Routing	Not included	Included
Accelerated SLAs	Not included	Included
Business Reviews & Strategic Planning	Not included	Included

*** Business hours** are defined as 9:00 AM to 5:00 PM in the hosting region (i.e., local time in Mumbai, India and/or North Virginia, USA, as applicable), excluding local holidays and weekends. These times may vary in countries with multiple time zones.

**** Designated Support Contacts:** Designated Support Contacts are named persons in Customer's organization who are authorized to submit tickets to Seclore Support and to work directly with Seclore's support team. Only Designated Support Contacts (*as defined in Section E below*) may submit tickets as well as receive status information with respect to Support Services.

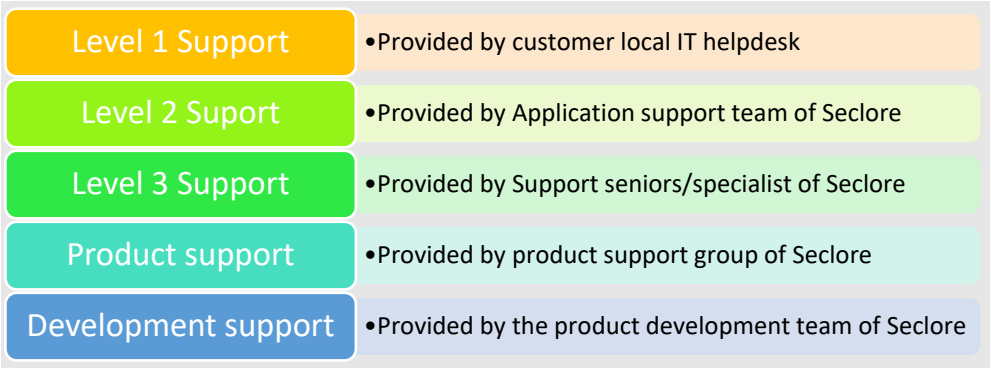
C. UPGRADES

1. Seclore will maintain the Seclore cloud environment and keep it upgraded with latest product releases. There will be a monthly maintenance window every second Saturday of the month where Services availability maybe limited or temporarily disrupted.

2. Customer will ensure that Software, if applicable and Seclore Agents are installed and maintained by Users and over-the-air upgrades will be pushed automatically through the Seclore portal as an when new releases are available.

D. USER SUPPORT:

1. **Support Levels**



2. Customer's local IT helpdesk ("***Helpdesk***") shall be responsible for providing Level 1 Support to Users. Training videos and knowledge bank to provide Level 1 Support will be available on Seclore portal at http://www.seclore.com/ adoption.seclore.com. The following terms outline Customer's Helpdesk responsibilities:
   - **i.** The Helpdesk will troubleshoot the incident and attempt to provide a resolution to the User.
   - **ii.** In the event Helpdesk is unable to provide a resolution, a Designated Support Contact shall raise a ticket, via the Designated Support Contact, to Seclore's support team, by visiting https://support.seclore.com/support/home. Seclore support team will acknowledge the ticket via e-mail and provide a ticket number to the Designated Support Contact.
   - **iii.** In order for Seclore's support team to resolve the incident, the Helpdesk shall document the incident and provide the following details to Seclore's support team:
     a. An accurate and complete description of the incident.
     b. Prioritization of the incident in accordance with Service Priority Definitions set forth in Table A below.
     c. The Helpdesk shall ensure that it captures enough information to allow Seclore to reliably reproduce the error that is the basis for the incident.

E. DESIGNATED SUPPORT CONTACTS:

1. Customer shall identify Designated Support Contact(s) and provide Seclore with the following details of such Designated Support Contact(s):
   i. Name
   ii. Designation
   iii. Email ID
   iv. Contact Number
2. Unless otherwise requested by Customer in writing, Seclore will only communicate with Customer's Designated Support Contacts with respect to resolution of support incidents. The Designated Support Contact(s) shall be responsible for providing additional information or remote sessions, as requested by Seclore, to enables Seclore's support term to troubleshoot the incident.
3. The number of Designated Support Contacts that Customer may appoint is dependent on the level of Support Services Customer has elected. A Designated Support Contact may be changed upon reasonable written notice to Seclore.

F. SERVICE LEVEL COMMITMENTS:

Seclore will respond to tickets based on the Service Priority as defined by Seclore in accordance with Table A below and respond to Customer in accordance with, Table B below. Escalation is from the Helpdesk to Seclore's 2nd level support team.

Table A

Service Priority Definitions

Service Priority	Description
Priority 1 (Critical business impact)	**Definition:** Priority 1 indicates that Customer is unable to use the Services, resulting in a critical impact on business operations. This condition requires immediate resolution. **Priority 1 Pre-requisite** – A Priority 1 issue has a crippling effect on Customer's business. i.e., the Seclore Policy Server is down. **Key Deliverables** – Priority 1 resolution involves reacting to Customer's emergency by immediately providing an appropriate resource ("**Analyst**"). Unless another agreement is in place, Priority 1 issues will be serviced on a continual effort basis until the Priority 1 condition has been resolved. Resolution of Priority 1 conditions may include temporary relief, enabling Customer's business to operate until a more comprehensive solution is provided. Priority 1 resolution shall be subject to the following conditions: • The Services, and the Customer, are eligible for Support Services • Affected functions of the Services must have already been successfully tested by Customer in User Acceptance Testing ("**UAT**") and were also working successfully in the past. • The Customer is available, as and when required and on a 24/7 basis, to actively collaborate with the Analyst and provide any information reasonably requested by the Analyst. • Access to Customer's systems or information about Customer's systems is available to the Analyst as and when requested, and on a 24/7 basis. • Once an alternative solution or workaround is provided, the Service priority level will be lowered by Seclore at its discretion. **Examples of Priority 1 case:** • A Policy Server deployed on hosting service provider's environment or Services deployed in customer environment has failed. • Multiple Users are unable to access the policy server on hosting service provider's environment. • The performance of the servers has degraded to an unusable level. • File is unrecoverable, corrupt, or lost. **Examples of cases that are not classified as Priority 1:** • The backend database is operational following a one–time outage; root cause analysis is required.

	• New feature Request or customization
Priority 2 (Significant business impact)	**Definition** - Priority 2 indicates the Services are usable but severely limited. **Priority 2 Pre-requisites:** • Services, or a part thereof, are returning an error or not responding. • Degraded performance is negatively impacting business operations, but an acceptable workaround exists. • Once an alternative solution or workaround is provided, the Service Priority level will be lowered by Seclore at its discretion. • Affected Product functions must have already been successfully tested during User Acceptance Testing and were also working successfully in the past. **Key Deliverables** – Priority 2 issues will be resolved during normal business hours, unless otherwise agreed in writing, and until the Priority 2 condition has been resolved. Priority 2 service delivery shall be subject to the following conditions: • Customer is available during normal business hours to collaborate with the Analyst and provides any information reasonably requested by the Analyst. • Access to the Customer's systems or information about Customer's systems is available to the Analyst as and when requested, during normal business hours. **Examples of Priority 2 case:** • Files are taking more time to open than usual. • Customer cannot access the Policy Server Portal. • Users can access Services, but access is slow, sometimes resulting in "page not found" messages or protected files not opening.
Priority 3 (Limited business impact)	**Definition** – Priority 3 indicates the Services are usable, but some features (which are not critical to operations) are unavailable. **Priority 3 Pre-Requisites:** • Issue is specific to one or a few Users. • Non-critical bugs are affecting the functioning of certain features. • Customer is able to access all Files. **Key Deliverables** – Priority 3 issues will be worked on during normal business hours, until the Priority 3 condition has been resolved. Priority 3 service delivery shall be subject to the following conditions: • Customer is available during normal business hours to collaborate with the Analyst and provides any information reasonably requested by the Analyst. • Access to the Customer's systems or information about Customer's systems is available to the Analyst as and when requested, during normal business hours.

	Examples of Priority 3 case: • Questions about how to use the features or functionality. • Feature Enhancement Request. • Usable performance degradation

Table B

Service Goals and levels by Plan

For the purpose of this Table B, response time shall be defined as the time elapsed between a ticket being raised by the Designated Support Contact and the assignment of a ticket number by Seclore's support team.

Priority	**Initial Incident Targeted Response Time**	
	Standard	**Gold**
P1 (High)	2 Business Hours	2 Hours
P2 (Normal)	8 Business Hours	4 Business Hours
P3 (Low)	3 Business Days	1 Business Day
Services Administration in Seclore Cloud		
System Health Monitoring	24/7	24/7
Uptime Guarantee *	99.5%	99.5%

* Subject to exclusions identified in Section 2(c)(ii)(b) of the Agreement.

G. OUT OF SCOPE

1. The following activities are outside the scope of Seclore Support Services:
   i. Maintenance and Support of the underlying infrastructure in the Customer's environment or any third party products procured by the Customer on which any Seclore component is installed or integrated with.
   ii. Resolution of issues arising due to problems in the Customer's underlying infrastructure e.g., database issues, network connectivity issues, data loss due to lack of availability of backed-up data, patching operating systems, physical machines, and hardware failure of the servers on which Seclore is installed.
   iii. Issues arising due to incompatibility with third party products which is not explicitly supported by Seclore will not be governed by the response timelines mentioned.
2. The following activities are **not** part of Standard Support Services unless explicitly agreed in the Order Form. Such activities will be initiated only as per availability of resources and may be subject to additional charges, such charges to be mutually agreed in writing between Customer and Seclore:
   i. Request for re-training and provision of custom documentation.
   ii. Request for resolving issues that arise due to improper installation by the customer's I.T team, failure to incorporate all upgrades, unauthorized/attempted modification, or alteration not performed by Seclore Support.
   iii. Onsite Support.
   iv. Migration of Customer tenant to a different hosting region supported by Seclore.

H. SUNSET PROVISIONS

1. As per Seclore's standard Product Life Cycle Policy, all Seclore provided components that are more than one (1) year old are automatically unsupported. This includes all Seclore Agents that are installed on end-user devices and server-side components like the Policy Server, Enterprise Application connectors, APIs, and SDKs. Please visit Seclore's Product Life Cycle Policy for more information.

2. Where the Services require a third-party product to operate (such as an operating system) or where the Services interoperates with a third party products (such as a Windows Office component) (collectively, "***Third Party Products***") and the Third-Party Product vendor withdraws generally available support for such product, then Seclore shall no longer support such Third-Party Product.

I. FAIR USAGE POLICY FOR CLOUD HOSTED INFRASTRUCTURE.

Customer's use of the Services is governed by the fair usage policy for the managed Seclore Rights Management infrastructure hosted by Seclore or its hosting service provider. Fair Usage Policy needs to be adhered to, to ensure that Seclore can provide the agreed service levels, for instance hosted on a shared infrastructure**.** Please visit Seclore's Fair Usage Policy for more information.

APPENDIX B

CONTROLLER-PROCESSOR DATA PROCESSING ADDENDUM [HOSTED]

This Controller-Processor Data Processing Addendum ("**DPA**") amends and/or is deemed fully incorporated into the Software Subscription Agreement (*together with any amendments, statements of work, attachments, schedules, exhibits, orders, the "Agreement"*) between the Customer and Seclore.

This DPA governs the Processing of certain Personal Data by Seclore on behalf of Customer, in accordance with applicable laws, and encompasses all activities related to provision of Software and/or Services under the Agreement. It includes in conjunction with the Agreement, documented instructions, specifying the subject-matter, duration, nature, and purpose of the Processing, establishing the rights and obligations of the Parties.

This DPA and the Agreement are Customer's complete instructions to Seclore, for the Processing of Personal Data.

1. Definitions and interpretation:

"Agreement"	means the Agreement to which this DPA is appended;
"Affiliate"	has the meaning set out in the Agreement;
"Customer"	has the meaning set out in the Agreement;
"Data Controller"	means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. *For the purposes of this DPA, the Data Controller shall be Customer;*
"Data Processor"	means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. *For the purposes of this DPA, the Data Processor shall be Seclore and any other third parties to which the Processing was delegated by Seclore;*
"Data Protection Legislation"	means (i) the GDPR (General Data Protection Regulation), *as defined below*, and the e-Privacy Directive (2002/58/EC); (ii) any applicable laws and/or regulations implementing the above legislation; (iii) all other applicable laws and regulations relating to the Processing of Personal Data and privacy; and (iv) the guidance and codes of practice issued by a relevant regulator;
"Data Subject"	means the Identified or Identifiable Natural Person to whom Personal Data relates;
"CCPA"	means California Consumer Privacy Act (as amended), Cal. Civ. Code §§ 1798.100 et seq. including any amendments and implementing regulations that become effective on or after the effective date of this DPA.
"EEA"	means the European Economic Area as defined under GDPR
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
"Identified or Identifiable Natural Person"	means a natural person (individual) who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person;
"Personal Data"	means any information relating to an Identified or Identifiable Natural Person and, for the purpose of the Agreement, this term includes (without limitation) any Personal Data Processed, by Seclore as a result of entering into or performing its obligations under the Agreement and any associated documents;
"Process", "Processed" or "Processing"	means 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;
"Seclore"	has the meaning set out in the Agreement;
"Sub-Processor"	means any third-party engaged by Seclore under this Agreement Processing Personal Data on behalf of Seclore including without limitation the sub-processors more particularly described in Annex III to Schedule 1.
"Supervisory Authority"	means the public authority monitoring implementation of GDPR as set out in Article 51 of GDPR.
"Authorized Users"	means both User and External User. "User" and "External User" have meanings set out in the Agreement;

Unless otherwise defined above, all capitalized terms used in this DPA will have the meaning given to them under the Agreement.

The terms and conditions of this DPA shall, in the event of conflict or inconsistency, with any other privacy-related documents, including privacy policies or privacy notices, take precedence over such documents.

2. Data Processing

2.1. The Parties acknowledge and agree that with regard to the Processing of Personal Data on behalf of Customer, Customer is the Controller and Seclore is a Processor to the extent it Processes Personal Data.

2.2. Customer is responsible for the accuracy, quality, and legality of the Personal Data Processed by Seclore, and the means by which Customer acquired the Personal Data.

2.3. Any Processing of Personal Data by Seclore under this DPA shall occur only:

2.3.1. on behalf and on the written instructions of Customer (including when Processing is initiated by Authorized Users);

2.3.2. in accordance with the Agreement;

2.3.3. for the purpose of fulfilment of Customer's written instructions; and

2.3.4. upon Customer procuring a valid consent from the Data Subjects for such Processing.

Seclore will Process Personal Data for the duration of the Agreement or as indicated in documented instructions from the Customer, unless otherwise agreed upon in writing or required by Applicable Law.

2.4. The types of Personal Data affected by the Processing within the scope of this DPA may include:

- Authorized User's name, email address;
- Authorized User's Internet Protocol (IP) addresses;
- Device name and Security Identifier (SID);
- Login identification;
- Authorized User agent type;
- Operating system;
- Date/time stamp of usage and activities performed with the File (access, close, edit, print, unprotect);
- Authorized User's device ID;
- Authorized User's folder name; and
- File Data

2.4.1. In case, any Personal Data is stored within the Files, such data is stored temporarily in Seclore's servers in encrypted form:

- For as long as Authorized Users access a File using agentless access this File is automatically deleted as soon as the Authorized User closes the browser session; and/or
- For as long as configured by the Customer.

2.4.2. In the event that Seclore provides remote Standard Support Services to Authorized Users, Seclore will collect the above-listed information in order to troubleshoot the incident and may be able to view Files open on the Authorized User's device.

2.5. Personal Data may be subject to the following basic Processing activities:

2.5.1. For the provision of the Services and / or Software contemplated under the Agreement (which includes enabling Customer to control and monitor information in the form of documents, emails, designs, and images);

2.5.2. For installation of the Software and creation of Authorized User accounts, to provide access to the Software;

2.5.3. For the provision of remote Standard Support Services to the Customer;

2.5.4. For analyzing aggregate usage patterns and trends; and

2.5.5. For monitoring compliance with the terms of this Agreement.

2.6. The categories of Data Subjects affected by the Processing of Personal Data on the behalf of Customer within the scope of this DPA will include:

2.6.1. Customer's employees / personnel designated as Authorized Users; and

2.6.2. Customer's prospects, clients, business partners, vendors, associates, and their respective personnel, and such other persons receiving the Files.

2.7. Sensitive and Special categories of data, including safeguards (if applicable):

☐ Health or medical data, including health care and payment/claims for health car	☐ Racial or ethnic origin	☐ Biometric or genetic data for the purpose of uniquely identifying a person
☐ Trade union membership	☐ Political opinions, religious or philosophical beliefs	☐ Information concerning a person's sex life or their sexual orientation
✓ None of the above		

Parties agree that Customer shall be solely responsible for compliance with any Data Protection Legislations as applicable to Controllers, including for any Personal Data that requires special handling or special categories of Personal Data such as, without limitation, that which relates to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, or personal finances.

2.8. Duration of Processing:

Between Seclore and Customer, the duration of processing will be determined by the Customer. However, if the customer doesn't specify the processing duration, it is the term of the subscription unless earlier deletion or return is requested in writing by the Customer, or for the duration of time Seclore is required to Process the Personal Data pursuant to the Agreement or applicable Data Protection Legislation.

Additionally, Seclore will retain the Personal Data for 90 days after the subscription term ends (the "Holding Period"). After the Holding Period expires, Seclore will destroy the data, or earlier upon the Customer's explicit written request.

3. General provisions:

3.1. Each Party will fully comply with all its obligations under the applicable Data Protection Legislation.

3.2. Seclore shall:

3.2.1. Process Personal Data only as necessary in the provision of the Services and/or Software as required pursuant to the Agreement; and

3.2.2. act only in accordance with the lawful and documented instructions of the Customer.

3.3. Personnel:

3.3.1. The Parties shall:

- ensure all employees involved in Processing or transferring of Personal Data have: (1) either committed themselves to confidentiality in writing or have statutory or fiduciary obligations; and (2) are authorized and appropriately trained to Process Personal Data;
- ensure the access to Personal Data is limited to the personnel necessary to execute the Party's obligations under the Agreement; and
- appoint a data protection officer, if required by Applicable Data Protection Legislation, and provide his / her contact details on written request to the other Party.

3.4. Technical and Organizational Measures:

3.4.1. Seclore will take appropriate technical and organizational security measures against the accidental or unlawful Processing of Personal Data and against the accidental or unlawful loss, destruction, alteration, unauthorized disclosure of, or access to, Personal Data. Seclore shall regularly test, assess, and evaluate the effectiveness of such technical and organizational measures for ensuring the security of the Processing.

3.5. Sub-Processing:

3.5.1. Customer gives Seclore a general authorization, as provided for in Article 28 of GDPR, to engage Sub-Processors to fulfill its obligations under the Agreement.

3.5.2. Such Sub-Processors that are third-party service providers are listed in Annex III to Schedule 1. Should Seclore add to or replace such Sub-Processors, Seclore shall give the Customer reasonable notice and an opportunity to object, provided such objection is based on reasonable grounds relating to data protection. If the Customer does not object within thirty (30) days, then such added or replaced Sub-Processors shall be considered incorporated into Annex III to Schedule 1 as an amendment to this DPA.

3.5.3. Seclore shall impose substantially similar data protection obligations on any Sub-Processors as set out in this DPA (in particular providing sufficient guarantees to implement appropriate technical and organizational measures). Seclore shall be liable for the acts and omissions of its Sub-Processors to the same extent Seclore would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

3.6. Data Transfers:

3.6.1. For any transfer of Personal Data from a country inside the European Economic Area, the United Kingdom, or Switzerland to a country outside the European Economic Area, the United Kingdom, or Switzerland, applicable requirements of GDPR must be fulfilled. Customer authorizes Seclore to store or Process Personal Data in the United States or any other country in which Seclore or its Sub-Processors maintain facilities. Customer authorizes Seclore to perform any such transfer of Personal Data to any such country and to store and Process Personal Data in order to provide the Software and/or Services or through documented instructions of Customer. The Parties will conduct all such activities in compliance with the Agreement, this DPA, and applicable Data Protection Legislation.

3.6.2. If Customer transfers Personal Data originating from the EEA to Seclore when Seclore is located in countries outside the EEA that have not received a binding adequacy decision by the European Commission, such transfers shall be made in compliance with applicable data transfer legal requirements and only by documented instructions from Customer. The

Parties acknowledge and agree to abide by the obligations set out in the Standard Contractual Clauses (European Commission Decision 2021/914 of 4 June 2021), found in Schedule 1, for any transfers of Personal Data from within the EEA to outside of the EEA. For the purpose of Processing Personal Data under this DPA and the incorporation of the Standard Contractual Clauses, Module 2 of the Standard Contractual Clauses shall be applicable.

3.7. CCPA:

3.7.1. To the extent that Seclore Processes any Personal Data relating to individuals who are California residents, Seclore shall comply with the CCPA. For the purposes of the CCPA, the Parties agree that Seclore is a "Service Provider" in the performance of its obligations, and that Customer is a "Business". As a Service Provider, Seclore shall not: (a) retain, use, or disclose any Personal Data: (i) for any purpose other than for the specific purpose of providing the Software and/or Services specified in the Agreement, including for a commercial purpose other than providing the Software and/or Services specified in the Agreement; (ii) outside of the direct business relationship between Seclore and Customer; or (iii) or as otherwise permitted by the CCPA; or (b) sell Personal Data. Finally, the transfer of the Personal Data to Seclore shall not be considered a "sale" as defined in the CCPA.

3.8. Privacy Impact Assessment:

3.8.1. Taking into account the nature of the Processing, if Customer believes or becomes aware that Seclore's Processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects as prescribed under applicable Data Protection Legislation, it shall promptly inform Seclore. Upon request and subject to payment of additional costs by the Customer, Seclore shall use commercially reasonable efforts to provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a privacy impact assessment and, if necessary, consult with any relevant data protection authority.

3.9. Rights of Data Subjects:

3.9.1. Seclore shall, to the extent permissible by applicable Data Protection Legislation, promptly notify Customer upon receipt of a request from a Data Subject to exercise any of the Data Subject's rights, including but not limited to the right of access, right to rectification, restriction of processing, right to be forgotten, data portability, objection to processing, or right not to be subject to automated individual decision making. Taking into account the nature of the Processing, Seclore shall, to the extent feasible, assist the Customer in fulfilling its obligations to respond to the Data Subject's request through suitable technical and organizational measures.

3.10. Audits:

3.10.1. Seclore shall, at Customer's expense, upon reasonable request of the Customer but only for cause and/or to the extent required by Article 28 of the GDPR, make available to Customer all relevant information necessary for audits or inspections, conducted by Customer, or an independent auditor appointed by the Customer (subject to such auditor not being competitor of Seclore and execution of a non-disclosure agreement) to demonstrate Seclore's compliance with the obligations under this DPA. Such audits or inspections shall be carried out only at Seclore's office premises and be limited to Seclore's Processing of Personal Data in its capacity as a Data Processor for the Customer only, not any other aspect of Seclore's business or information systems or its other clients.

3.10.2. If the Customer requires Seclore to submit to audits or inspections, Customer will provide Seclore with at least sixty (60) days advance written notice of such audit or inspection. Such written notice will specify the things, people, places, or documents to be made available. Anything produced by Seclore during such audit or inspection will only be in connection with the Customer's engagement with the Customer and will not include any information pertaining to Seclore's other clients. Further, such information produced for inspection will be considered Seclore's Confidential Information and, notwithstanding anything to the

contrary in the Agreement, will remain Confidential Information in perpetuity or the longest time allowable by applicable Data Protection Legislation after termination of the Agreement.

3.10.3. Seclore may allow for onsite audit or inspection requests at Customer's expense, only in cases where, (a) Seclore has not provided sufficient written evidence of its compliance with the technical and organizational measures; (b) a Security Breach has occurred; (c) an inspection is officially requested by Customer's Supervisory Authority; or (d) applicable Data Protection Legislation provides Customer with a mandatory on-site inspection right; and provided that Customer shall not exercise this right more than once per year unless the applicable Data Protection Legislation requires more frequent inspections. Such facility inspections shall be conducted in a manner that does not impact the ongoing safety, security, commitments to other clients by Seclore, confidentiality, integrity, availability, continuity, and resilience of the inspected facilities, nor otherwise expose or compromise any confidential data Processed therein.

3.11. Security Breach

3.11.1. In the event of an unauthorized or accidental use, disclosure or access of Personal Data or any other breach of this DPA by Seclore or any of its staff, Sub-Processors, or any other identified or unidentified third party ("**Security Breach**"), Seclore shall promptly notify the Customer in writing upon the discovery and confirmation of such Security Breach, without undue delay.

3.11.2. Such notification shall contain, at least:

- a description of the nature of the Security Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
- the details of a contact point where more information concerning the Personal Data breach can be obtained; and
- the likely consequences and the measures taken or proposed to be taken to address the Security Breach, including mitigate its possible adverse effects.

3.11.3. Where, and insofar as, it is not possible to provide all the above information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

3.11.4. Seclore shall take all necessary and legally required corrective or mitigating actions, to remedy or mitigate any Security Breach; and

3.11.5. Seclore shall not make any announcement or publish or otherwise authorize any broadcast of any notice or information about the Security Breach without notifying Customer unless legally required to do so.

3.12. Cooperation with Supervisory Authorities:

3.12.1. In the event of reporting and notification obligations to Supervisory Authorities and/or affected Data Subjects arising from Security Breaches, the Parties shall, upon request, extend reasonable support and furnish information to the other Party to facilitate the investigation of any Security Breach and to fulfill any legally mandated obligations.

4. Miscellaneous

4.1. This DPA may be amended, supplemented, or replaced by Seclore in written or otherwise documented form at any time by notifying the Customer through the email address provided by the Customer in the Agreement.

If Seclore cannot delete or return the Personal Data due to legal or regulatory requirements, Seclore will immediately inform Customer and will take all necessary steps to ensure that the Personal Data concerned is kept confidential subject to such legal or regulatory requirements and will not be further Processed.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the Personal Data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of Personal Data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e); and

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

[INTENTIONALLY OMITTED]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the Personal Data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the Personal Data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and Personal Data, the data exporter may redact a part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all Personal Data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all Personal Data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to that data (hereinafter '**Personal Data breach'**). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the Personal Data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management, and monitoring of the contract. It shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a Personal Data breach concerning Personal Data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the Personal Data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise, or defence of legal claims in the context of specific administrative, regulatory, or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) General Written Authorisation: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data

exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the Personal Data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority

of one of the Member States in which the data subjects whose Personal Data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the Personal Data by the data importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical, or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the Personal Data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall

promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses, where:

(i) the data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its

entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of Personal Data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Ireland.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

---

1 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of Personal Data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

2 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein, and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

3 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

4 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently

representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The data exporter is the identified as Controller in Section 1 of this DPA.

Data importer(s): The data importer is the Seclore entity identified as Processor in Section 1 of this DPA.

Address: Plot No 07 & 08, Excom House, Off Saki Vihar Road, Sakinaka, Andheri (East) Mumbai 400072

Email: DPO@seclore.com

Contact Details: Abhijit Tannu, CTO; Tuhina Chakrabarty, Director – Legal

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred:

1. Customer's employees / personnel designated as Authorized Users; and

2. Customer's prospects, clients, business partners, and vendors etc.

Categories of Personal Data transferred:

The types of Personal Data affected by the Processing within the scope of this DPA may include:

- Authorized User's name, email address;
- Authorized User's Internet Protocol (IP) addresses;
- Device name and Security Identifier (SID);
- Login identification;
- Authorized User agent type;
- Operating system;
- Date/time stamp of usage and activities performed with the File (access, close, edit, print, unprotect);
- Authorized User's device ID;
- Authorized User's folder name; and
- File Data

In case, any Personal Data is stored within the Files, such data is stored temporarily in Seclore's servers in encrypted form:

- For as long as Authorized Users access a Files using agentless access and this document is automatically deleted as soon as the Authorized User closes the browser session; and / or
- For as long as configured by the Customer.

In the event that Seclore provides remote Standard Support Services to Authorized Users, Seclore will collect the above-listed information in order to troubleshoot the incident and may be able to view Files open on the Authorized User's device.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

No sensitive data transferred.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

As necessary for the purposes of processing according to the Agreement.

Nature of the processing:

1 Fulfilment of the purpose of the Agreement.

2. Seclore may also utilize Anonymized Information for purposes of improving Seclore's products and services. "Anonymized Information" means Personal Information that has been sufficiently anonymized, deidentified, or aggregated so that it cannot identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular Data Subject, device, or the Customer, provided that Seclore: (i) has implemented technical safeguards that prohibit reidentification of the Data Subject to whom such information may pertain; (ii) has implemented business processes that specifically prohibit reidentification of such information; (iii) has implemented business processes to prevent inadvertent release such information, and (iv) makes no attempt to reidentify such information.

Purpose(s) of the data transfer and further processing:

1. For the provision of the Services contemplated under the Agreement (which includes enabling Customer to control and monitor information in the form of documents, emails, designs, and images);

2. For creation of Authorized User accounts, to provision access to Services and/or the Software (if applicable); and

3. For the provision of remote Standard Support Services to the Customer.

4. For analysing aggregate usage patterns and trends.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

Subject to Section 2 of the DPA, Seclore will retain Personal Data for as long as required for fulfilling the purpose under the Agreement, unless: (i) a longer retention period is required for audit, legal, or regulatory purposes; or (ii) Customer instructs Seclore in writing to: (a) keep certain Personal Data longer; or (b) return certain Personal Data earlier.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing:

See Annex III

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

_____ [To be populated at a later stage] _____

ANNEX III

LIST OF SUB-PROCESSORS

Seclore engages Sub-Processors who have, or potentially will have access to or Process Personal Data on behalf of Seclore.

Below table lists downs the names and various functions performed by the Sub-Processors

Sub-processor	Description of Processing	Hosting Location(s)	Applicable Data Protection Terms
Amazon Web Services, Inc.	Cloud infrastructure hosting	U.S.	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Fresh Desk	Support ticketing platform	U.S.	https://www.freshworks.com/legal/

Unless otherwise specified above, the nature and duration of each Sub-Processor's activity is the following:

Nature: Assisting Seclore in fulfilment of the purpose of the Agreement.

Duration: Term of the Seclore's agreement with the Sub-Processor unless earlier deletion or return is requested by Seclore. For additional information please see "Applicable Data Protection Terms" in the table above.

Sub-processor Security

Seclore assesses the security posture of all Sub-Processors before use and periodically thereafter to validate that the Sub-Processor implements a security program in accordance with Seclore's security policy for the categories of Personal Data Processed by the Sub-Processor. Further, Seclore establishes contractual safeguards with its Sub-Processors through data processing agreements.