



### SUBSCRIPTION SERVICES AGREEMENT

This Subscription Services Agreement (this “**Agreement**”) is entered into on [redacted] by and between **Varonis Systems, Inc.**, a Delaware corporation, having its principal place of business at 801 Brickell Ave, 8<sup>th</sup> Floor, Miami, FL 33131 (“**Varonis**”) and [redacted], a [redacted] corporation, with a principal place of business at [redacted] (“**Subscriber**”).

**WHEREAS**, Varonis holds proprietary rights of certain Subscription Services; and **WHEREAS**, subject to the terms of this Agreement, Varonis agrees to grant Subscriber a limited right to access and use the Subscription Services and provide Subscriber with certain Services in connection with the Subscription Services; **NOW, THEREFORE**, in consideration of the conditions contained herein, the parties, intending to be legally bound, agree as follows:

**IN WITNESS WHEREOF**, the parties hereto have caused this Agreement to be executed by their respective authorized representatives. This Agreement may be executed in any number of counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.

<p>[Subscriber to complete full legal name]</p> <p>By:</p> <p>Title:</p> <p>Date:</p>	<p>Varonis Systems, Inc.</p> <p>By:</p> <p>Title:</p> <p>Date:</p>
---	--

Approved by Varonis Legal

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

## TERMS AND CONDITIONS

1. **DEFINITIONS.** Any capitalized terms used in this Agreement that are not otherwise defined shall have the meaning as set forth below:

1.1 **“Additional Services”** means services which are supplemental or ancillary to Subscriber’s use of the Subscription Services as may be offered by Varonis to Subscriber from time to time, including without limitation, professional services, penetration testing services and forensic services.

1.2 **“Affiliate”** means any entity which directly or indirectly controls, is controlled by or is under common control with the subject entity, where “control” means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.3 **“Allotted Usage”** means the permitted usage scope of the Subscription Services purchased by the Subscriber.

1.4 **“Documentation”** means Varonis’ product documentation detailing the operation and use of the Subscription Services, as generally made available to Varonis’ subscribers, and as updated from time to time by Varonis.

1.5 **“Fees”** has the meaning ascribed thereto in Section 8 hereof.

1.6 **“Intellectual Property Rights”** means all intangible legal rights, titles and interests including without limitation, all inventions, patents, patent applications, trademarks, service marks, trade dress, logos, trade names, and corporate names, domain names, any work of authorship, copyrights, trade secrets, Confidential Information (as defined below), and all other proprietary rights in whatever form or medium, in each case, on a worldwide basis; together with all revisions, extensions, reexaminations translations, adaptations, derivations, and combinations thereof and including all goodwill associated therewith.

1.7 **“Order”** means the purchase order or other ordering document that Varonis accepts from Subscriber or a Varonis authorized reseller (**“Reseller”**) which lists the products and services to

be provided by Varonis. If Subscriber is purchasing through a Reseller, the Order will be between Varonis and the Reseller while the Subscriber will have a separate purchasing document that Subscriber enters into directly with the Reseller that will apply to Subscriber’s purchase from that Reseller. The Order, and the products and services included therein, shall be subject to the terms of this Agreement.

1.8 **“Services”** means Support Services and Additional Services.

1.9 **“Subscriber Data”** means electronic data generated in the course of the use of the Subscription Services and the Services.

1.10 **“Subscriber Program”** means the object code form of the service application made available to Subscriber to be installed on Subscriber’s computing device/environment and used solely in connection with the Subscription Services.

1.11 **“Subscription Services”** means Varonis’ web-based cloud solution that is offered on a software-as-a-service basis. For the purpose of this Agreement, the Subscriber Program, and any Updates thereto (as defined in the SLA), shall be considered an integral part of the Subscription Services.

1.12 **“Support Services”** means the provision of Updates and technical support by Varonis pursuant to its SLA as further detailed in Section 3.

1.13 **“Term”** has the meaning ascribed thereto in Section 9.1 hereof.

## **2. SUBSCRIPTION SERVICES.**

2.1 Subject to the terms and conditions of this Agreement, including the Subscriber’s payment of all applicable Fees when due, Varonis grants Subscriber a non-exclusive, non-transferrable, non-sublicensable, limited license to access and use the Subscription Services during the subscription period set forth in the applicable Order. The Subscription Services may be accessed solely for Subscriber’s internal business purposes, in

accordance with the Documentation, and for the Allotted Usage purchased by Subscriber.

2.2 Subject to the terms and conditions of this Agreement, including Subscriber's payment of all applicable Fees when due, Varonis grants Subscriber a non-exclusive, nontransferable, non-sublicensable, limited license, to: (a) install the Subscriber Program solely in Subscriber's computing device/environment; and (b) during the subscription period set forth in the applicable Order, use the Subscriber Program solely as required for using the Subscription Services in accordance with this Agreement.

2.3 Subscriber may allow its Affiliates to access and use the Subscription Services on its behalf, provided that any such use shall be in accordance with this Agreement, and Subscriber shall remain fully responsible for any such use.

2.4 If Subscriber's actual usage of the Subscription Services exceeds the Allotted Usage (the "**Over Usage**"), Subscriber will be notified of the Over Usage and the parties shall discuss in good faith the reason for such Over Usage. If Varonis determines that the Over Usage is consistent and exceeds the Allotted Usage, Varonis shall notify Subscriber and Subscriber's Allotted Usage shall be updated to reflect and cover Subscriber's actual usage of the Subscription Services. In such event, Subscriber shall be required to pay the associated subscription fees for the updated Allotted Usage for the remaining portion of the subscription term.

### **3. SUPPORT AND ADDITIONAL SERVICES.**

3.1 Varonis shall provide Subscriber with Support Services in connection with the Subscription Services, all subject to the terms of this Agreement and Varonis' standard support principles, which is attached hereto as Exhibit A ("**SLA**"), provided that any such update shall not adversely and materially affect Subscriber's rights.

3.2 Varonis may provide Subscriber, from time to time, with certain Additional Services. Unless otherwise acknowledged or agreed by the parties on a case-by-case basis, all Additional Services shall

be subject to the terms and conditions of this Agreement.

3.3 If Subscriber purchases the Varonis SaaS Managed Data Detection and Response Services ("**MDDR**"), Subscriber's use of the MDDR shall be subject to the Varonis MDDR Services Agreement, a current version of which is attached hereto as Exhibit B.

### **4. RESTRICTIONS AND RESPONSIBILITIES.**

4.1 Subscriber shall not (and shall not permit others to) do any of the following with respect to the Subscription Services: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, lend, distribute, time share, operate as a service bureau, or otherwise make any of the Subscription Services available for access by third parties; (ii) conduct any security scanning and/or penetration testing or use the Subscription Services in any way which is not in accordance with this Agreement, or in a way which adversely affects other subscribers and their use of the Subscription Services; (iii) make any commercial use of the Subscription Services or grant any third party any right to use the Subscription Services, whether or not for any consideration; (iv) access or use the Subscription Services for developing or operating products or services intended to be offered to third parties; (v) disassemble, reverse engineer, decompile, or otherwise attempt to derive the source code, algorithms or technology included in the Subscription Services; (vi) copy, create derivative works based on, or otherwise modify the Subscription Services; (vii) remove or modify a copyright, trademark, logo or other proprietary rights notice or brand labeling in the Subscription Services; (viii) externally publish or release any benchmarking or performance data, or comparative study or analysis, applicable to the Subscription Services; (ix) circumvent, disable or otherwise interfere with security-related or access-related features of the Subscription Services; (x) represent that it possesses any proprietary interest in the Subscription Services; or (xi) directly or indirectly, take any action to contest Varonis' Intellectual Property Rights in the Subscription Services or infringe them in any way. Subscriber

represents, covenants, and warrants that Subscriber will use the Subscription Services solely in compliance with this Agreement, the Documentation and all applicable laws and regulations.

4.2 Subscriber shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect, access to or otherwise use the Subscription Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, and web servers (collectively, "**Equipment**"). Subscriber shall also be responsible for maintaining the security of the Equipment, Subscriber's account(s), password(s) (including but not limited to administrative and user passwords) and files, and for all uses of Subscriber's account or the Equipment. Under no circumstances shall Varonis be liable for any Equipment and/or services used by Subscriber to connect, access or otherwise use the Subscription Services.

4.3 Subscriber is solely responsible for all activity occurring in and through the Subscription Services by the Subscriber and anyone on its behalf. Subscriber shall use its best efforts to prevent unauthorized access to, or use of, the Subscription Services and will notify Varonis immediately, and in any event within 48 hours, in case of any unauthorized use of any password or account or any other known or suspected breach of security or privacy rights.

4.4 Subscriber shall be solely responsible for ensuring that its use of the Subscription Services complies with all applicable laws (including, all privacy laws), rules, and regulations.

4.5 Subscriber acknowledges that the Subscription Services are subject to the United States Financial Sanctions Regulations and the U.S. Export Administration Regulations. Subscriber further agrees that it will comply with all financial sanctions and export control laws, regulations, and orders administered by the U.S. Government and/or, to the extent consistent with U.S. antiboycott law, comparable controls imposed by other governments having jurisdiction over

activities under this Agreement (collectively, "**Trade Control Laws**") to assure that the Subscription Services are not exported, re-exported, transferred, installed or accessed, directly or indirectly, in violation of such Trade Control Laws. Subscriber warrants that neither Subscriber nor any party/ies that individually or in the aggregate own 50% or more of the Subscriber, nor, to the best of Subscriber's knowledge, any party authorized by Subscriber to use the Subscription Services, is subject to financial sanctions or other restriction on receipt of goods or services imposed by applicable Trade Control Laws (collectively, "**Restricted Parties**") and agrees that it shall be deemed a material breach if Subscriber violates Trade Control Laws in connection with activity under this Agreement, or becomes a Restricted Party, or otherwise becomes subject to applicable restrictions under Trade Control Laws, whether such restrictions apply to Subscriber or to the region in which Subscriber is located, including any restrictions that result in a requirement not to use License Exception ENC and to instead obtain an export license or similar government authorization to supply Subscriber with products or services. Subscriber agrees to reasonably cooperate and assist Varonis or any of its representatives with an audit, review or investigation of Subscriber's compliance with applicable laws and regulations as set forth in this Section. In connection with such review, audit or investigation, Subscriber will deliver to Varonis all relevant records, information and documents reasonably requested by Varonis, and any such information shall be deemed as Subscriber's Confidential Information. Subscriber will immediately rectify non-compliance as requested by Varonis. The foregoing is without derogating from any other right or remedy Varonis may have under this Agreement or under any applicable law. Notwithstanding Section 9.2, a breach by Subscriber of this Section shall entitle Varonis to terminate the Agreement and any rights granted hereunder immediately, upon notice to Subscriber. To the extent permitted by applicable law and in Varonis' reasonable discretion, informed by its assessment of the risk arising from the circumstances of the breach, instead of immediate

termination, Varonis may provide Subscriber with 10 business days to cure the breach to Varonis' satisfaction.

4.6 Subscriber shall notify Varonis in writing if any Subscriber content is subject to the International Traffic in Arms Regulations ("ITAR") or is subject to the Export Administration Regulations ("EAR") and classified under an Export Control Classification Number ("ECCN") that is controlled for reasons other than Anti-Terrorism ("AT"). In such event, Varonis shall take appropriate actions to ensure compliance with applicable Trade Control Laws. Absent prior written notification, Subscriber shall be deemed the exporter of such Subscriber content resulting from use of the Subscription Services and Services.

## 5. INDEMNIFICATION.

5.1 Subscriber hereby agrees to defend, indemnify, and hold Varonis and its Affiliates, and their directors, officers, shareholders, employees and agents harmless against any and all judgments, damages, losses, liabilities, settlements, costs and expenses (including, without limitation, reasonable attorneys' fees) (collectively, "Loss(es)") in connection with any third party claim brought against the indemnified parties that arises from a claim that the Subscriber Data or the use thereof in connection with the Subscription Services infringes or misappropriates a third party's privacy rights or applicable laws.

5.2 Varonis shall indemnify, defend and hold Subscriber and its Affiliates, and their directors, officers, shareholders, employees and agents harmless from and against all Losses arising from any demands, claims or legal action by any third party based upon any claim that the Subscription Services infringe intellectual property right of such third party ("Varonis' IP Indemnity"). Varonis' IP Indemnity shall not extend to claims based on: (i) an unauthorized modification of the Subscription Services made by Subscriber where the Subscription Services would not be infringing without such modification, or (ii) Subscriber's combination of the Subscription Services with a

third-party product unless the combination was contemplated in the Documentation; or (iii) Subscriber's use of the Subscription Services other than in accordance with the terms of this Agreement.

5.3 If the Subscription Services become the subject of an indemnification claim, Varonis shall use reasonable efforts, at Varonis' option and sole expense to either: (i) procure for Subscriber the right to continue to use the Subscription Services as contemplated hereunder, or (ii) modify the Subscription Services to eliminate any claim which might result from its use hereunder, provided that the Subscription Services' performance must remain at least as good as provided in the Documentation, or (iii) replace the Subscription Services with equally suitable, compatible and functionally equivalent non-infringing subscription services, at no additional charge to Subscriber. If the remedies in sub-sections (i)-(iii) are not commercially practicable, as shall be determined by Varonis, Subscriber shall cease using the Subscription Services and be entitled to a pro-rated refund of any pre-paid Fees for the remaining, unused portion of the subscription period. The remedies in Section 5.2 are exclusive with respect to any claim of infringement raised in connection with the Subscription Services.

5.4 The indemnified party will (x) provide the indemnifying party with a written notice of the claim, (y) grant the indemnifying party sole control over the defense and settlement of the claim (except that the indemnifying party may not settle any claim without the indemnified party's prior consent, which shall not be unreasonably withheld, except for a monetary settlement which fully releases the indemnified party), and (z) provide the indemnifying party reasonable assistance, at indemnifying party's expense.

## 6. CONFIDENTIALITY.

6.1 During the Term, each party may be provided with certain non-public technical, financial, proprietary, confidential or trade secret information or data of the other party, which given the totality of the circumstances, a reasonable

person or entity should have reason to believe is proprietary, confidential, or competitive (the “**Confidential Information**”). Without limitation from the generality of the above said, Confidential Information shall include sensitive information, including without limitation, any information identified as confidential, information about the Subscription Services, the Subscriber Program, Documentation, roadmap, information related to Varonis’ business, products, internal practices and any proprietary or sensitive information of Varonis. Confidential Information shall exclude any information that the receiving party can demonstrate (i) is now or subsequently becomes generally available in the public domain through no fault or breach on the part of receiving party; (ii) was in the rightful possession or known by the receiving party prior to disclosure by the disclosing party; (iii) receiving party rightfully obtained, without restrictions, from a third party who has the right to transfer or disclose it, without default or breach of this Agreement and/or any other confidentiality obligations; or (iv) the receiving party has independently developed, without breach of this Agreement or any use of or reference to the disclosing party’s Confidential Information.

6.2 The receiving party agrees: (a) not to disclose the disclosing party’s Confidential Information to any third parties other than to its Affiliates and their directors, officers, employees, advisors or consultants (collectively, the “**Representatives**”) on a strict “need to know” basis only, and provided that such Representatives are bound by written agreements to comply with the confidentiality obligations as protective as those contained herein; (b) not to use or reproduce any of the disclosing party’s Confidential Information for any purposes except to carry out its rights and responsibilities under this Agreement; (c) to keep the disclosing party’s Confidential Information confidential using at least the same degree of care it uses to protect its own Confidential Information, which shall in no event be less than a reasonable degree of care. The receiving party shall remain liable at all times for any breach of this Section by any of its Representatives.

6.3 Notwithstanding the foregoing, if any Confidential Information is required to be disclosed by law, order of a court or by an administrative body, to the extent legally permissible, the receiving party shall notify disclosing party promptly and in writing of such required disclosure and shall reasonably cooperate with the disclosing party, at the disclosing party’s reasonable request and expense, in any lawful action to contest or limit the scope of such required disclosure and its efforts to seek a protective order or other appropriate relief.

6.4 The receiving party acknowledges and agrees that the disclosing party may suffer financial and other loss and damage if any Confidential Information is disclosed except as permitted by this Agreement, and that monetary damages alone may be an insufficient remedy for any such breach. The receiving party agrees that the disclosing party, in addition to any other right or remedy that it may have available to it at law or in equity, will have the right to seek and obtain immediate injunctive relief in any court of competent jurisdiction to prevent a breach of this Section and to compel specific performance with regard to this Section.

6.5 The parties’ obligations with respect to Confidential Information shall expire five years following termination or expiration of this Agreement unless a longer period of protection applies under applicable law.

## **7. PROPRIETARY RIGHTS; PRIVACY.**

7.1 Varonis owns and will retain all right, title, and interest, including all Intellectual Property Rights, in and to the Subscription Services, the Services, and the Documentation. This Agreement does not convey to the Subscriber any interest or right in or to the Subscription Services, Services or Documentation.

7.2 Subscriber, or its licensors, own and retain all right, title, and interest in and to the Subscriber Data.

7.3 Subscriber hereby grants to Varonis a worldwide, perpetual, irrevocable, royalty-free, fully paid-up license to use any questions,

comments, suggestions, ideas, feedback to the extent provided by Subscriber in connection with the Subscription Services or the Services (“**Feedback**”) for any business purpose determined by Varonis, including for incorporating the Feedback into Varonis’ products and services.

7.4 Subscriber Data may include Personal Data (as defined in the DPA) that is made available by Subscriber in connection with the Subscription Services and Services. Such Personal Data is processed pursuant to the terms of the Data Processing Addendum attached hereto as Exhibit C (“**DPA**”). The DPA is considered an integral part of this Agreement.

## **8. PAYMENT OF FEES.**

Subscriber will pay Varonis or its Reseller, as applicable, the fees for the Subscription Services and Services (the “**Fees**”). In the event Subscriber purchases the Subscription Services and/or Services directly from Varonis (and not through a Reseller), then the Parties shall negotiate in good faith the applicable provisions related to payment terms, pricing, taxes, and invoicing procedures in connection with such purchase.

## **9. TERM AND TERMINATION.**

9.1 This Agreement shall commence on the Effective Date and shall remain in effect until expiration of the last Order issued hereunder, unless terminated earlier as provided in Section 9.2 herein (the “**Term**”). Each Order shall remain in effect for the fixed subscription term set forth in such Order.

9.2 In addition to any other remedies a party may have, each party may terminate this Agreement upon thirty (30) days’ written notice to the other party, if the other party materially breaches any of the terms or conditions of this Agreement and does not cure such breach within a thirty (30) days’ notice period. Notwithstanding: (i) if Subscriber breaches any of its obligations in Section 4.1 of this Agreement, and such breach is not curable (as shall be determined by Varonis reasonably and in good faith) Varonis reserves the right to terminate this Agreement immediately;

and (ii) any non-payment shall be considered a material breach of this Agreement by Subscriber.

9.3 Upon termination or expiration of this Agreement: (i) Subscriber shall immediately cease using the Subscription Services; and (ii) only to the extent that this Agreement is terminated by Varonis in accordance with this Agreement, any outstanding Fees set forth in the Order shall become immediately due and payable.

9.4 In addition to any of its other rights or remedies (including, without limitation, any termination rights) set forth in this Agreement, Varonis reserves the right to suspend the Subscription Services and/or Services if: (a) Varonis deems such suspension necessary as a result of Subscriber’s breach of Sections 4.1 or 4.5, (b) Varonis reasonably determines that such suspension is necessary to avoid material harm to Varonis or its other subscribers, including without limitation, if the Subscription Services are experiencing denial of service attacks, mail flooding, or other attacks or disruptions beyond Varonis’ control, or (c) such suspension is required by law or at the request of governmental entities having jurisdiction.

9.5 All sections of this Agreement which by their nature are intended to survive termination or expiration of the Agreement, including, without limitation, accrued rights to payment, and Sections 1, 4, 6, 7, 8, 9, 10.2, 11, 12 and 13 will survive termination or expiration of this Agreement.

## **10. WARRANTIES AND DISCLAIMER.**

10.1 Each party represents and warrants that this Agreement constitutes a legal, valid, and binding obligation, enforceable against it in accordance with the terms of this Agreement. Further, Varonis warrants that during the subscription period set forth in the applicable Order, the Subscription Services will conform in all material respects to the Documentation. Varonis’ sole liability and Subscriber’s exclusive remedy for any breach of this performance warranty shall be to remedy or replace any such non-conformance in accordance with the SLA. Varonis further represents and warrants that the Services will be

performed by Varonis in a professional and workmanlike manner. The foregoing warranty will not apply if the non-conformance was caused by (i) use of the Subscription Services other than in accordance with the Documentation and this Agreement, including, without limitation, any accident and/or abuse, (ii) the Subscriber's failure to properly maintain the Subscription Services in accordance with the instructions provided by Varonis, (iii) modifications to the Subscription Services by Subscriber or any third-party, or (iv) third-party hardware, software, or services used in connection with the Subscription Services, including the Equipment.

10.2 EXCEPT FOR THE WARRANTIES SPECIFICALLY SET FORTH IN THIS AGREEMENT, VARONIS DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICES OR THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, THAT ALL ERRORS WILL BE CORRECTED OR THAT THEY SHALL MEET THE SUBSCRIBER'S REQUIREMENTS; NOR DOES VARONIS MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SUBSCRIPTION SERVICES OR THE SERVICES. THE SUBSCRIPTION SERVICES ARE NOT INTENDED TO BE USED AS A STORAGE, BACKUP OR ARCHIVING SERVICE. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SUBSCRIPTION SERVICES AND THE SERVICES ARE PROVIDED "AS IS" AND VARONIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

#### **11. LIMITATION OF LIABILITY.**

11.1 NEITHER PARTY SHALL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO, UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY OR PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING COST OF PROCUREMENT OF SUBSTITUTE GOODS, LOSS OF BUSINESS OR REVENUE, LOSS OF GOODWILL, COMPUTER FAILURE OR MALFUNCTION AND LOST PROFITS; OR

(B) FOR ANY AMOUNTS THAT EXCEED THE FEES RECEIVED BY VARONIS FOR THE SUBSCRIPTION SERVICES DURING THE 12 MONTHS PERIOD PRECEDING THE EVENT THAT GAVE RISE TO THE CLAIM, IN EACH CASE, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES. IN SUCH JURISDICTIONS, THESE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY.

11.2 The limitations set forth in Section 11.1(B) above will not apply with respect to damages occasioned by: (A) the willful misconduct or fraud of a party; (B) claims that are the subject of Subscriber's indemnification obligations under Section 5.1 of this Agreement and Varonis' IP Indemnity; or (C) Subscriber's breach of its obligations under Sections 4.1 or 4.5.

#### **12. EVALUATION; PRIVATE PREVIEW; "BETA" VERSION.**

12.1 Varonis may, at its sole discretion, grant Subscriber a limited right to: (i) access the Subscription Services or a part thereof and provide Subscriber with free of charge Additional Services related to such limited access, and/or (ii) use new features, functionalities, platforms, modules or services developed by Varonis, if presented as part of "private preview" and/or "beta" versions, as further detailed in the SLA, in each case, for trial and evaluation purposes (the "**Evaluation Subscription**") and for a period to be determined by Varonis (the "**Evaluation Period**"). Any Evaluation Subscription may be used by Subscriber at its sole discretion. Varonis may extend the Evaluation Period at its sole discretion. Any such Evaluation Subscription will be: (i) on an as-is basis, without warranties of any kind, including without any obligation to provide Services to Subscriber, (ii) without any liability whatsoever, and (iii) except as set forth in this Section 12, subject to the terms of this Agreement. Upon the termination or expiration of the Evaluation Period, Subscriber will cease using the Evaluation Subscription to which Subscriber was granted access. Subscriber hereby agrees to receive communications from Varonis for

promotional and support purposes during the Evaluation Period and thereafter.

### 13. MISCELLANEOUS.

13.1 **Publicity.** Subject to Subscriber's prior written approval, Varonis may refer to Subscriber as a customer of Varonis and include Subscriber's name and logo, including, without limitation, as part of its public filings, and/or in marketing materials (including in a list of its customers) and/or on Varonis' web site. Neither party may issue any press release regarding this Agreement without the other party's prior written consent nor use the name or logo of the other party.

13.2 **Severability.** If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

13.3 **Assignment.** This Agreement is not assignable, transferable or sublicensable by Subscriber except with Varonis' prior written consent, which shall not be unreasonably withheld or delayed. Varonis may transfer and assign this Agreement and/or any of its rights and/or obligations under this Agreement without consent.

13.4 **No Agency.** No agency, partnership, joint venture, or employment is created as a result of this Agreement and Subscriber does not have any authority of any kind to bind Varonis in any respect whatsoever.

13.5 **Notices.** All notices given under this Agreement shall be in writing and shall be deemed to have been duly given when delivered, if delivered by messenger during normal business hours of the recipient; when sent, if transmitted by email transmission (receipt confirmed and with a confirmation copy sent by post) during normal business hours of the recipient; or on the third business day following posting, if posted by international air mail. Notices to Varonis shall be sent to: 801 Brickell Ave, 8<sup>th</sup> Floor, Miami, FL 33131, USA; Attn: Varonis Legal Department,

legal@varonis.com. Notices to you shall be sent to the Subscriber's Address.

13.6 **Third Party Software.** The Subscription Services may contain software provided by third parties. The restrictions contained in this Agreement shall apply to all such third-party software providers and third-party software as if they were Varonis' and the Subscription Services, respectively. In addition, some of the Subscription Services may contain software provided by Oracle, Inc. ("**Oracle**"). Such Subscription Services are subject to Oracle provisions which are attached hereto as Exhibit D, in addition to those provisions contained in this Agreement.

13.7 **Law and Jurisdiction.** All disputes arising out of, or relating to, this Agreement shall be governed and construed in accordance with the law of the State of New York, excluding such state's conflicts of law rules. Any legal action of whatever nature by or against a party arising out of, or relating to, this Agreement shall be brought solely in either the federal or state courts located in New York, New York. The parties hereby consent to (and waive any challenge or objection to) personal jurisdiction and venue in the above-referenced courts. Notwithstanding the foregoing, each party may seek equitable relief in any competent jurisdiction in an action for protection of its Intellectual Property Rights or Confidential Information. The United Nations Convention on Contracts for the International Sale of Goods, Uniform Commercial Code, and the Uniform Computer Information Transaction Act (UCITA) are expressly excluded from this Agreement.

13.8 **Force Majeure.** Varonis shall not be responsible or liable for any loss, damage, delay or failure to act(s) caused by any circumstances beyond Varonis' reasonable control ("**Force Majeure**"), including, without limitation, war, invasion, insurrection, riot, the order of any civil or military authority, fire, flood, earthquake, weather, interruption to or absence of energy supplies, strikes, other labor disputes, the failure of Varonis' suppliers or carriers to meet their contractual obligations, issues related to external applications,

telecommunications, internet service providers, hosting facility failures, cyber-attacks and government promulgation of applicable financial sanctions or export controls.

**13.9 High Risk and Restricted Data Activities.** The Subscription Services are not fault-tolerant and are not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Subscription Services could lead directly to death, personal injury, or severe physical or environmental damage, or similar federal or state data security statutes (collectively, “**High Risk and Restricted Data Activities**”). Varonis and its suppliers specifically disclaim any express or implied warranties of fitness for High Risk and Restricted Data Activities.

**13.10 Disaster Recovery Plan; Business Continuity Plan.** Varonis shall maintain, according to industry standards, a disaster recovery plan and a business continuity plan.

**13.11 U.S. Federal Government End User Provisions.** If any part of the Subscription Services is acquired by or on behalf of a unit or agency of the U.S. Government (a “**US Governmental Entity**”), such US Governmental Entity agrees that the Subscription Services and all related Documentation are “commercial computer software” or “commercial computer software documentation” and that, absent a written agreement to the contrary, the US Governmental Entity’s rights with respect to the Subscription Services and the related Documentation are governed by the terms of this Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

**13.12 Amendments.** This Agreement may not be amended except by a written agreement signed by authorized representatives of both parties.

**13.13 Exercise of Rights.** Varonis may exercise its rights and obligations under this Agreement

through its wholly owned subsidiaries. Varonis shall be responsible for any acts or omissions of its subsidiaries in the performance of this Agreement as if such acts or omissions were its own.

**13.14 Entire Agreement.** This Agreement, including all documents referred to herein, represents the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior written and oral understandings between the parties, including any interim agreements executed by the parties and including any non-disclosure agreement(s) entered by the parties.

**13.15 Consent to Conduct Business Electronically.** The parties understand and agree that, notwithstanding anything herein to the contrary, their electronic signature (including, without limitation, by typing their name at the end of an email confirming agreement, acceptance or consent) manifests their consent to be bound by all terms and conditions set forth in this Agreement.

**13.16 Reseller Orders.** Subscriber may procure the Subscription Services and the Services directly from a Reseller pursuant to a separate agreement with Reseller that includes the Reseller order form and other terms (a “**Reseller Arrangement**”). Varonis will be under no obligation to provide the Subscription Services and the Services to Subscriber as a result of a Reseller Arrangement if Varonis has not received an Order from such Reseller. Subscriber acknowledges that Reseller is not authorized to make any changes to this Agreement or otherwise provide any warranties, representations, promises or commitments on behalf of Varonis or in any way concerning the Subscription Services or the Services. If Subscriber procured the Subscription Services and/or Services through a Reseller Arrangement, then Subscriber agrees that Varonis may share certain Subscriber Data with Reseller in relation to Subscriber’s Allotted Usage of the Subscription Services and the Services. If Subscriber has procured the Subscription Services and/or Services through a Reseller, Subscriber acknowledges that the termination provisions in this Agreement will apply if the Reseller fails to timely pay the applicable Fees

to Varonis due to Subscriber's failure to timely pay to the Reseller.

#### 13.17 TRIBAL SUBSCRIBERS

**Representation of Subscriber Authority.** The execution, delivery and performance by Subscriber of this Agreement and the obligations contained herein have been duly authorized by all necessary tribal governmental and other action, and do not require any consent or approval not heretofore obtained of any tribal officer or tribal body.

**Limited WAIVER OF SOVEREIGN IMMUNITY.** Subscriber hereby clearly, expressly, unequivocally and irrevocably waives its sovereign immunity in any forum provided for in this agreement in connection with any dispute arising under this Agreement, including as set forth in Paragraph

13.7. Subscriber consents to the jurisdiction of the federal and state courts in Paragraph 13.7. Varonis and its successors and assigns shall be entitled to all available legal and equitable remedies, including the right to specific performance, money damages and injunctive or declaratory relief. Subscriber agrees that it shall not plead or raise as a defense to any action brought by Varonis or its successors or assigns any right or claim of right to the requirement of exhaustion of tribal court remedies prior to the commencement of litigation proceedings, even if any such tribal forum would have concurrent jurisdiction over any such dispute but for such waiver. Subscriber waives its rights to have any dispute heard in any tribal court or before any other trial tribunal, forum, council or other adjudicative body whether or not such forum now exists or is hereinafter created.

## Exhibit A

# Varonis' Service Level Agreement

This Service Level Agreement, as may be amended from time to time by Varonis (“**SLA**”) describes the Support Services and applies to all subscribers who have paid the applicable Fees. This SLA is part of and governed by the terms of the subscription services agreement governing Subscriber’s use of the Subscription Services (the “**Agreement**”). In the event of a conflict between the terms of this SLA and the terms of the Agreement, the terms and conditions of this SLA shall control. Capitalized terms not defined in this SLA shall have the meaning assigned to them in the Agreement.

### A. Scope of Support Services

\*

1. The Support Services include the following:

\*

- web based and telephone support for installation and general use questions;
- access to Varonis’ Support Portal, Knowledgebase and Subscriber Community
  - Creation, update and managing Subscriber’s support cases online
  - Unlimited Knowledge Base access
  - Unlimited access to technical documents;
- use of Varonis’ dedicated toll-free number (<https://www.varonis.com/services/support>); and
- two Subscriber’s named contacts.

\*

2. Provision of Updates; Supported Versions of the Subscriber Program.

\*

- Varonis shall make available to Subscriber Updates of the Subscriber Program, if and when Varonis makes such Updates generally available to its other subscribers. Notwithstanding Varonis’ obligations hereunder or under the Agreement, Varonis shall have no responsibility or liability of any kind arising out of, or resulting from, Subscriber’s failure to correctly and timely install the Updates. Varonis will provide Support Services under this SLA only for the current and available version of the Subscriber Program. For the purpose hereof, “**Updates**” means new versions, modifications, work around, upgrades, patches, error-correction, improvements, fixes, releases hotfixes, service packs, feature packs, in each case, which are designed and released by Varonis to optimize and/or repair the operation of the Subscriber Program. Updates shall not include any new functionality, features or modules offered by Varonis as separate or additional products, components or add-ons. All Updates are subject to the terms and conditions of the Agreement.
- Each Version of the Subscriber Program shall be supported for as long as such Version is the current Version and for an additional six (6) months period after the release of the next Version (for example, Version 1.4 shall be supported for as long it is the current Version and for six (6) months after the release of Version 1.5 (even if subsequent Versions were released during such six (6) months period).

\*

\*“**Version**” shall mean a subsequent release of a Subscriber Program and its associated Documentation denoted by a change in the first and/or second numeral of the Subscriber Program’s release number (e.g., a change from v.1.3.3 to v.2.0 or from v.1.4 to v.1.5). “**Versions**” shall not include new functionalities, features or modules offered by Varonis as separate or additional products, components or add-ons.

\*

3. Hours of Operation and Contact Information.

Regional Hours of Operations:

**North America:** Monday–Friday, 09:00-21:00 EST, for a list of observed holidays, click [here](#)

**EMEA:** Monday–Friday, 09:00-21:00 CET, for a list of observed holidays, click [here](#)

**APAC:** Monday–Friday, 06:00-18:00 China Standard Time, for a list of observed holidays, click [here](#)

Each Subscriber may choose only one of the time zones identified above for the Support Services (if no time zone is chosen by the Subscriber, Varonis will set the time zone based on the address listed in the purchase order issued to Varonis). Such time zone shall dictate the hours of support provided by Varonis irrespective of the location(s) in which the Subscriber Program is installed and/or the territories from which the Subscription Services are used by Subscriber.

Contact Support: <http://www.varonis.com/services/support/>

4. The Support Services do not include the following:

- operating systems and third-party applications;
- alterations or revisions to the Subscription Services made by the Subscriber or third parties;
- use of the Subscription Services other than as authorized in the Agreement;
- use of any Subscription Services that has been announced as End of Life (including unsupported Versions of the Subscriber Program).
- escalations from Subscriber personnel other than the Subscriber’s named contacts;
- issues with respect to which Varonis has provided corrections that were not implemented by the Subscriber; or data requested from Subscriber which was not provided in a timely manner;

\*Subscription Services and Additional Services rendered as part of an Evaluation Subscription, beta versions, private preview features or technology or other offerings available on an early access or private preview basis. Varonis may, at its sole discretion, (i) change or discontinue any beta versions or private preview features, at any time and without notice to subscribers; (ii) choose not to release a beta version and/or private preview feature into “General Availability,” and (iii) charge fees for beta versions and private preview features, if fully released;

- any migration services; and
- issues of performance when the Subscriber’s environment does not meet Varonis’ sizing recommendations as provided to Subscriber, or as set forth in the Documentation.

\*

**B. Availability; Service Credits**

\*

1. Availability. Varonis will use commercially reasonable efforts to assure that Subscriber is able to access the Varonis’ web application of the Subscription Services at least 99% of the time, as measured by Varonis over the course of twelve (12) months period(s) (the “**Availability**”). In the event that Varonis does not meet the Availability commitment set forth herein, Subscriber will be eligible to receive a Service Credit as described below.

\*

\*Availability Exclusions. The Availability commitment does not apply to any performance or availability issues which resulted from or which are related to any of the following: (i) Scheduled Maintenance - planned downtime of which Varonis provides at least three (3) days’ notice to Subscriber, except for planned downtime of up to 30 minutes during the weekend hours, for which notice shall not be required. Varonis

will use commercially reasonable efforts to schedule all planned downtime during the weekend hours; (ii) **Unscheduled Maintenance** – maintenance required to prevent and/or address substantial harm to the Subscription Services. To the extent practicable, Varonis shall use reasonable efforts to notify Subscriber of any emergency maintenance; (iii) **Force Majeure event(s)**; (iv) **Subscriber’s**, an authorized user’s or any other third-party’s actions or inactions, including, without limitation, Subscriber’s failure to properly set up and operate the Subscription Services in accordance with the Agreement, issues resulting from Subscriber’s equipment, connectivity, software or hardware, Subscriber’s failure to comply with its obligations in Section (D) Below, or the performance of any security scanning and/or penetration testing by Subscriber; and (v) Varonis’ exercise of its rights under the Agreement or under applicable law, including suspension or termination of Subscriber’s right to use the Subscription Services in accordance with the Agreement.

2. **Service Credits.** Service Credits apply in any calendar year in which the Availability falls within the ranges set forth in the table below.

<b>Annual Availability Percentage</b>	<b>Service Credit Percentage</b>
Less than 99% but greater than or equal to 97%	2% of Applicable Fee
Less than 97% but greater than or equal to 95%	4% of Applicable Fee
Less than 95% but greater than or equal to 93%	8% of Applicable Fee
Less than 93% but greater than or equal to 90%	10% of Applicable Fee
Less than 90%	20% of Applicable Fee

3. **Credit Request and Payment Procedures.** In order to receive a Service Credit, Subscriber must submit a claim by opening a case with Varonis technical support within thirty (30) days after the end of the calendar year during which the Availability commitment was not met, which must include: (i) the words “SLA Credit Request” in the subject line; (ii) the calendar year for which Subscriber is claiming Service Credits together with the dates and times of each incident of claimed non-Availability; and (iii) logs or other information evidencing the failure to meet the Availability (any confidential or sensitive information should be removed or redacted). Subscriber’s failure to open the case with the information required above will disqualify Subscriber from receiving a Service Credit. If Varonis confirms the Availability was not met, then Varonis will issue Subscriber a note confirming that Varonis will apply the applicable Service Credit towards Subscriber’s next invoice.

**\*Maximum Credits; Dispute Resolution.** Service Credits will not entitle Subscriber to any refund or other payment from Varonis. Service Credits may not be transferred or applied to any other account. The aggregate maximum Service Credits to be issued to Subscriber for any and all incidents in which Availability was not met will not exceed 20% for each annual subscription period. This SLA states Subscriber’s sole and exclusive remedy for any failure by Varonis to meet the Availability commitment herein. If a dispute arises with respect to this SLA, Varonis will make a determination in good faith based on its system logs, monitoring reports, configuration records, and other available information. Varonis, at its reasonable discretion, will make such information available for review by Subscriber at Subscriber’s reasonable prior written request, on a case-by-case basis, subject to appropriate privacy and security protections.

**C. Error Severity Levels and Response Time**

<b>Error Severity Level</b>	<b>Description</b>	<b>Contact Method</b>	<b>Response Time*</b>

<b>Severity 1</b>	A down situation where core component(s) of the Subscription Services is/are non-operational and there is no known work-around	Notify Support via portal or phone	up to 2 hours, during the Hours of Operation chosen by the Subscriber
<b>Severity 2</b>	A major component of the Subscription Services is not functioning and no work-around is available, but the Subscription Services still supports core functionality		up to 4 hours, during the Hours of Operation chosen by the Subscriber
<b>Severity 3</b>	A minor component of the Subscription Services is not functioning		24 hours, during the Hours of Operation chosen by the Subscriber

\* Response Time: the time between Subscriber’s initial contact and the acknowledgment response by Varonis. To qualify for the above response times, Subscriber is required to cooperate with Varonis in providing reproducible results for errors reported.

**Escalation Procedures.** Varonis’ escalation procedures raise the visibility of Subscriber’s most important issues internally. Varonis may, at its discretion, pass any issue into the escalation process. Varonis’ standard escalation process includes evaluating the severity level of the issue. Varonis’ goal is to address issues in a timely manner taking into consideration the severity of the issue. In general, if Subscriber is not satisfied with a response from the Technical Support staff, Subscriber may request that the issue will be escalated to a Support Team Lead or to the Director of Technical Support. Once an issue is escalated, Varonis Technical Support will coordinate a call or a meeting with Subscriber’s resources for gathering relevant data required to identify and address the issue. Subscriber shall provide adequate resources and the requested data in a timely manner in order to enable Varonis to best address the issue.

**D. Subscriber Obligations**

In order for Varonis to provide the Support Services, Subscriber shall (i) ensure the readiness and appropriate conditions of its hardware, computerized systems and environment; (ii) cooperate with Varonis’ requests which may include, without limitation, enabling Varonis to remotely access the relevant systems and environments (including the Subscriber Program) and provide Varonis with the required permissions and configurations; (iii) provide all available information about a reported error(s) and take all such reasonable measures requested by Varonis in order to detect and provide further information with respect to each error, and (iv) ensure that its contacts authorized to receive the Support Services are fully available and knowledgeable with respect to the Subscription Services and capable of receiving remote instructions from Varonis.

**Exhibit B**

**Varonis SaaS Managed Data Detection and Response Services**

This Varonis SaaS Managed Data Detection and Response Services Agreement (“Agreement”) is governed by the terms of the Subscription Services Agreement between Varonis and Subscriber (the “SaaS Agreement”). All capitalized terms used herein and not otherwise defined shall have the meanings assigned to them in the SaaS Agreement. In case of any conflict between the terms of this Agreement and the SaaS Agreement, this Agreement shall prevail.

1. Scope of Services. Subject to the terms and conditions of this Agreement, Varonis will provide Subscriber with cybersecurity managed data detection and response services solely with respect to Varonis’ built-in threat models and solely with respect to the platforms licensed by Subscriber and supported by the Subscription Services (the “Services”). The Services are intended to assist Subscriber improve its security posture and risk reduction by identifying risks, emerging threats and vulnerabilities. The Services may only be used by Subscriber internally and may not be shared with any third party. The Services are provided by Varonis remotely and shall only be available during periods in which Subscriber has ongoing, duly paid, Subscription Services. In addition, the Services are not provided for Varonis DA Cloud platform and threat models. Key components of the Services, as may be updated by Varonis from time to time, are detailed in the table below.

Key Component	Elements
Onboarding	<ul style="list-style-type: none"> <li>*Service initiation meetings (kick off meeting followed by operational sessions to ensure MDDR readiness)</li> <li>*Review of Subscriber IT Environment</li> <li>*Varonis’ MDDR license enablement</li> <li>*Subscriber to provide contact details on its behalf</li> </ul>
Detection and Investigation	<ul style="list-style-type: none"> <li>*Ongoing monitoring and investigation of security alerts generated by Varonis’ SaaS platform.</li> <li>*Varonis would contact Subscriber if sufficient evidence has been collected by Varonis to deem a threat as malicious.</li> <li>*Varonis would contact subscriber if further input were required to proceed with the investigation.</li> <li>*Varonis may conduct threat hunting across the Subscriber’s IT environment for relevant indicators of compromise and tactics collected from current incident response engagements. Threat hunting activities are limited to Subscriber Data gathered through the Subscription Services. Varonis will inspect collected Subscriber telemetry to detect activity, such as the presence of persistence mechanisms, anomalous user activity, threat actor tactics, anomalous network communications, and anomalous application usage.</li> <li>*Investigation starts following the completion of the MDDR onboarding phase.</li> </ul>
Response	<ul style="list-style-type: none"> <li>*Varonis will initiate threat response actions to contain an attack or a threat (i.e., disable a user, block IP addresses, etc.). In addition, Varonis will provide recommendations for remediation of the effected environment. For clarification, Varonis will not be providing any remediation services. Subscriber is and shall remain solely and fully responsible for determining which of Varonis’ recommendations, if any, should be accepted and implemented. Varonis will not decide or determine what actions or remediations should be enforced by Subscriber.</li> </ul>

	<p>*Once the onboarding process is completed, Varonis will provide access to incident response and security experts 24x7x365.</p> <p>*Response time shall be determined by criticality. Business critical requests that may have severe and immediate impact on Subscriber's environment shall be responded within 2 business hours.</p> <p>*Response to any other requests for consultation will be provided within 1 business day.</p>
--	--

All services which are not specifically set forth above are not included as part of the Services and are out of scope for this Agreement.

2. Availability. All monitoring and investigation will be provided on a 24/7/365 basis.
3. Investigation Service Level Targets. The following service level targets are utilized to provide Subscriber with guidelines around timing expectations for investigation, excluding threat hunting. The SLA is measured from the time a security alert was raised to the time an investigation started.

*Ransomware	*30 minutes
*Other security alerts	*2 hours

4. Subscriber Cooperation and Responsibilities. Subscriber agrees to fully cooperate with Varonis in a timely manner as necessary for Varonis to perform the Services hereunder. Such cooperation shall include, without limitation, the following responsibilities which Subscriber shall be required to comply with: (i) Subscriber must provide Varonis access to all required environments as needed by Varonis to provide the Services; (ii) Subscriber must be present or provide a Subscriber-nominated representative who will be present and available for all planning and review sessions; (iii) Subscriber must participate, as Varonis reasonably deems appropriate, in the provision of the Services; (iv) Subscriber understands that without proper participation, including goal setting, the Varonis technician cannot work towards meeting Subscriber's needs or performing the Services as outlined above; (v) Subscriber will cooperate with and follow the instructions given by Varonis analysts; (vi) Subscriber shall provide information and assistance (e.g., files, logs, IT environment context) promptly during investigations that Varonis conducts in relation to threats against Subscriber; (vii) Subscriber shall identify and authenticate all users authorized to use the Services; (viii) Subscriber shall apply controls against unauthorized access by users, and maintain the confidentiality of usernames, passwords and account information Subscriber understands that without prompt and adequate cooperation as set forth above, Varonis will not be able to perform the Services or, if performed, the Services may be materially altered or delayed.
5. Limited Warranty. Varonis undertakes to provide the Services in accordance with the terms hereof and in a professional and workmanlike manner. EXCEPT FOR THE ABOVE UNDERTAKING, AND IN ADDITION TO THE DISCLAIMER OF WARRANTIES IN THE SAAS AGREEMENT, WHICH SHALL APPLY IN FULL FORCE AND EFFECT TO THE SERVICES HEREUNDER, WHILE THE SERVICES ARE INTENDED TO ASSIST SUBSCRIBER TO IDENTIFY AND REDUCE CERTAIN RISKS, IT IS IMPOSSIBLE TO COMPLETELY ELIMINATE RISKS, AND VARONIS MAKES NO GUARANTEE THAT THE SERVICES OR THE USE THEREOF SHALL IDENTIFY, REMEDIATE OR PREVENT ALL MALWARE, MALICIOUS SOFTWARE, INTRUSIONS, COMPROMISES, THREATS, INCIDENTS, VULNERABILITIES OR ANY OTHER UNAUTHORIZED ACTIVITY IN THE SUBSCRIBER'S ENVIRONMENT AND SUBSCRIBER SHALL NOT HOLD VARONIS RESPONSIBLE THEREOF. FURTHER, VARONIS IS AND SHALL NOT BE LIABLE FOR ANY ACTIONS TAKEN AT THE DIRECTION OF SUBSCRIBER HEREUNDER.

SUBSCRIBER AGREES AND ACKNOWLEDGES THAT VARONIS WILL NOT BE LIABLE OR BE CONSIDERED IN BREACH OF THIS AGREEMENT (INCLUDING ANY APPLICABLE SLA): (I) DUE TO

ANY DELAY OR FAILURE TO PERFORM ITS OBLIGATIONS HEREUNDER AS A RESULT OF INDUSTRY OR INFRASTRUCTURE WIDE RANSOMWARE, CYBERWARFARE OR OTHER CYBERATTACKS THAT CAUSE A SECURITY SERVICES TEAM TO BE UNABLE TO PROVIDE RESOURCES TO ADDRESS AN INCIDENT IN A TIMELY MANNER; (II) DUE TO A FORCE MAJEURE EVENT; (III) DUE TO LEGAL PROHIBITION, INCLUDING PASSING OF A STATUTE, DECREE, REGULATION, OR ORDER; (IV) DURING ANY PERIOD OF SUSPENSION BY VARONIS OR DURING ANY PERIOD IN WHICH VARONIS' AVAILABILITY COMMITMENT DOES NOT APPLY, IN ACCORDANCE WITH THE TERMS OF THE SAAS AGREEMENT AND THE SLA; OR (V) IF SUBSCRIBER IS IN BREACH OF THE SAAS AGREEMENT OR THIS AGREEMENT (INCLUDING WITHOUT LIMITATION, IF SUBSCRIBER IS OVERDUE ON ANY PAYMENTS).

**Exhibit C**  
**CUSTOMER DATA PROCESSING ADDENDUM FOR SAAS PRODUCTS**

This Data Processing Addendum (“**DPA**”) forms an integral part of the Agreement (“**Main Agreement**”) between Varonis Systems, Inc. and/or its subsidiaries. (“**Company**”) and between the counterparty agreeing to these terms (“**Customer**”; each “**Party**” and together “**Parties**”) and applies to the extent that Company processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Main Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA

**All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement.**

**1. Definitions**

- 1.1 "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).
- 1.2 "**Data Protection Law**" means, as applicable, any and all domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (as amended, and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 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 (“**GDPR**”); the Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (“**UK GDPR**”); Singapore’s Personal Data Protection Act 2012 (No. 26 of 2012) (“**PDPA**”) and Personal Data Protection Regulations 2021, and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (“**CCPA**”) and the regulation enacted thereunder including the California Privacy Rights and Enforcement Act of 2020 (“**CPRA**”); Australia's Privacy Act 1988 including the Australian Privacy Principles (“**APPs**”); the Virginia Consumer Data Protection Act, Va. Civ. Code § 59.1 (“**VCDPA**”) (together with the CCPA and CPRA, “**US Data Protection Laws**”), including any amendments or replacements to the foregoing.
- 1.3 “**Data Subject**” means an individual to whom Personal Data relates. Where applicable, Data Subject shall be deemed as a “**Consumer**” as this term is defined under the US Data Protection Laws and as an “Individual”, as this term is defined under the PDPA.
- 1.4 “**DPF**” means the EU-U.S. Data Protection Framework, pursuant to the European Commission Implementing Decision of 10.7.2023 (“**EU-U.S. DPF**”), and, as applicable, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework.

- 1.5 "EEA" means those countries that are member of the European Economic Area.
- 1.6 "Permitted Purposes" mean any purposes in connection with Company performing its obligations under the Main Agreement.
- 1.7 "Security Incident" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the avoidance of doubt, any Personal Data Breach (as defined under Data Protection Laws) will comprise a Security Incident.
- 1.8 "Security Measures" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company's business, the level of sensitivity of the data collected, handled and stored, and the nature of Company's services, as further described in Annex 2 (that can be found in the following link: <https://varon.is/securityschedule>).
- 1.9 "Standard Contractual Clauses" mean (a) with respect to the transfers to which the GDPR applies - Module Two or Module Three, as applicable, of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4th 2016, as available here: [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en); and (b) with respect to transfers to which the UK GDPR applies - the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018, currently available here: <https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf>; both (a) or (b) above, as applicable, are incorporated herein by reference.
- 1.10 "Sub-Processor(s)" mean any Affiliate, agent or assignee of Company that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by Company.
- 1.11 "UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, which was entered into force on 21 March, 2022.
- 1.12 The terms "Controller", "Personal Data", "Processor", "Process" and "Processing" shall have the meanings ascribed to them in the Data Protection Law, as applicable.

## 2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

- (A) Company processes Personal Data that is made available by the Customer in connection with the Main Agreement (whether directly by the Customer or indirectly by a third party retained by and operating for the benefit of the Customer);
- (B) The Data Protection Law apply to the processing of Personal Data.

2.2 This DPA will only apply to the services for which the Parties agreed to in the Main Agreement ("**Services**"), which incorporates the DPA by reference.

### 3. **Parties' Roles**

3.1 In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller (as well as, as applicable, the Business, as the term is defined under US Data Protection Laws, or the Organization, as this term is defined under the PDPA) and Company is a Processor (as well as, as applicable, the Service Provider, as this term is defined under US Data Protection Laws, or the Data Intermediary, as this term is defined under the PDPA), or if the Personal Data processed by the Company in accordance with the Main Agreement is of a Customer acting as Processor of behalf of a third party, then the Company shall be the Sub Processor. Accordingly:

- (A) Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;
- (B) The Parties acknowledge that the Customer discloses Personal Data to Company only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, Customer warrants to Company that Customer's instructions and actions with respect to the Personal Data, including its appointment of Company as Sub-Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant controller.

3.3 Notwithstanding anything to the contrary in the DPA, Customer acknowledges that Company shall have the right to Process certain Personal Data collected in the context of providing the Services, for its legitimate business purposes as a Controller, such as:

- (A) the provision and operation of its Services, administrating the business and/or contractual relationship with the Customer, billing, audit and recordkeeping purposes, as well as for account management, security, establishment or exercise of legal claims and protection against fraudulent or illegal activity.
- (B) for the purpose of improving customers' threat protection. If the Customer wishes that the Company uses only aggregated and/or anonymized information for such purposes, Customer is solely responsible to choose to opt-out of non-aggregated and/or non-anonymized processing in the management interface in the Customer's product. The Company may use aggregated and/or anonymized information for any purpose, subject to the confidentiality obligation in the Main Agreement. For the avoidance of doubt, non-aggregated and non-anonymized data referred to in this section shall be retained for the same period as the Personal Data.

### 4. **Compliance with Laws**

4.1 Each Party shall comply with its respective obligations under the Data Protection Law.

- 4.2 Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.
- 4.3 Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.
- 4.4 Throughout the duration of the DPA, Customer agrees and warrants that:
- (A) Personal Data has been and will continue to be processed by Customer in accordance with the relevant provisions of the Data Protection Law;
  - (B) Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Company and shall provide Company only instructions that are lawful under Data Protection Law;
  - (C) The processing of Personal Data by Company for the Permitted Purposes, as well as any instructions to Company in connection with the processing of the Personal Data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and that
  - (D) The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained the relevant consents or lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions and the Permitted Purposes).

## 5. **Processing Purpose and Instructions**

- 5.1 The subject matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, shall be as set out in the Main Agreement, or in the attached Annex 1, which is incorporated herein by reference.
- 5.2 Company shall Process Personal Data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Main Agreement and the Data Protection Law, unless Company is otherwise required by law to which it is subject (and in such a case, Company shall notify Customer of that legal requirement before Processing, provided that the Company is not legally prohibited from doing so).
- 5.3 To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Main Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions.
- 5.4 Company shall not retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the Parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under Data Protection Law. Company's performance of the Services may include disclosing Personal Data to Sub-Processors where this is necessary for the performance of the

Services. The Company certifies that it, and any person receiving access to Personal Data on its behalf, understand the restrictions contained herein.

## **6. Reasonable Security and Safeguards**

- 6.1 Company represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data Processed by Company in connection with the Main Agreement, and (ii) to protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2 (that can be found in the following link: <https://varon.is/securityschedule>).
- 6.2 The Security Measures are subject to technical progress and development and Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result, in the Company's discretion, in the material degradation of the overall security of the services procured by Customer. The Company will provide notice (in the Company's portal for customers) of material changes in Security Measures, when possible, at least 10 days before the change will take effect.
- 6.3 Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who Processes Personal Data. Company shall ensure that persons authorized to Process Personal Data are under an appropriate obligation of confidentiality.

## **7. Security Incidents**

- 7.1 Upon becoming aware of a Security Incident, Company will notify Customer without undue delay and will provide reasonable information relating to the Security Incident as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Security Incident as relates to Company's products and services.

## **8. Security Assessments and Audits**

- 8.1 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company.
- 8.2 At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with Company's SOC 2 Type II report, so that Customer can reasonably verify Company's compliance with its obligations under this DPA. Customer shall rely on the SOC 2 Type II report for validation of proper information security practices and shall not have an additional right to audit Company's compliance unless such right is specifically granted to Customer under applicable law. The foregoing shall not apply solely in the case of a Security Breach resulting in a material business impact to Customer or in connection to a Supervisory Authority specific request. In such event, Customer shall provide Company with 30 days prior written notice (insofar as possible) and the details of any 3<sup>rd</sup> party auditor on its behalf, for approval.

## 9. Cooperation and Assistance

- 9.1 If Company receives any requests from individuals or applicable data protection authorities relating to the Processing of Personal Data under the Main Agreement, including requests from individuals seeking to exercise their rights under Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. The Customer is responsible for verifying that the requestor is the data subject whose information is being sought or its duly authorized representative. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.
- 9.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Company shall be entitled to provide such information.
- 9.3 Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by Company in connection with its provision of such assistance.
- 9.4 Upon reasonable notice, Company shall:
- (A) Taking into account the nature of the Processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;
  - (B) Provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails material costs or expenses to Company, the Parties shall first come to agreement on Customer reimbursing Company for such costs and expenses.

## 10. Use of Sub-Processors

- 10.1 Customer provides a general authorization to Company to appoint Sub Processors in accordance with this Clause.
- 10.2 Company may continue to use those Sub Processors already engaged by Company as at the date of this DPA, as specified in Annex 3 (that can be found in the following link: <https://varon.is/subprocessors>), subject to Company, in each case as soon as practicable, meeting the obligations set out in this DPA.
- 10.3 Company can at any time appoint a new Sub-Processor provided that the Company provides notice (in the Company's portal for customers), at least 10 days before the appointment will take effect, and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must

contain reasonable and documented grounds relating to a Sub-Processor's non-compliance with Data Protection Law. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Sub-Processor. Where Company notifies Customer of its intention to continue to use the Sub-Processor in these circumstances and does not provide the Customer with any other alternative, Customer may, by providing written notice to Company, terminate the Services in the Main Agreement that require the Processing by that Sub-Processor.

10.4 With respect to each Sub-Processor, Company shall ensure that the arrangement between Company and the Sub-Processor is governed by a written contract, including terms which offer at least the same level of protection as those set out in this DPA and meet the requirements of Data Protection Law, including the requirements of article 28(3) of the GDPR, as applicable;

10.5 Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA.

10.6 Company will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Company's behalf.

## **11. Transfer of EEA or UK Residents' Personal Data outside the EEA or UK**

11.1 The Company has certified with the DPF and shall comply with its principles with respect to any personal data transfers outside the EU, UK or Switzerland, to the US. To the extent that Company Processes Personal Data outside the EEA, UK or an Approved Jurisdiction, which is not subject to Company's DPF certification, then the Parties shall be deemed to enter into the Standard Contractual Clauses, subject to any amendments contained in Exhibit A, in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein).

11.2 Company may transfer Personal Data of residents of the EEA or UK outside the EEA or UK ("**Transfer**"), only subject to the following:

(A) The Transfer is necessary for the purpose of Company carrying out its obligations under the Main Agreement, or is required under applicable laws; and

(B) The Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to appropriate safeguards (for example, through the use of the Standard Contractual Clauses, or other applicable frameworks), (iii) in accordance with the DPF principles, or (iv) in accordance with any of the exceptions listed in the Data Protection Law (in which event, Customer will inform Company which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies).

11.3 Annex 3 to this DPA (that can be found in the following link: <https://varon.is/subprocessors>) provides a list of countries to which the Personal Data will be transferred by Company under this DPA.

## **12. Data Retention and Destruction**

12.1 Company will only retain Personal Data for the duration of the Main Agreement or as required to perform its obligations under the Main Agreement, for the establishment or exercise of legal claims, or as otherwise required to do so under applicable laws or regulations. The retention policy can be found in

the Company's Software Privacy Policy - <https://www.varonis.com/software-privacy-policy>. Following expiration or termination of the Main Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Main Agreement, except to the extent Company is required under applicable laws to retain the Personal Data.

### **13. Obligations under US Data Protection Laws**

- 13.1 To the extent that Company processes Personal data of which is subject to the US Data Protection Laws:
- 13.2 Company shall not sell or share such Personal Data (as the terms "sell" and "share" are defined under US Data Protection Laws).
- 13.3 Company is prohibited from retaining, using or disclosing such Personal Data for a commercial purpose other than providing the service to the Customer under the Main Agreement and from retaining, using or disclosing such Personal Data outside of the Main Agreement, including but not limited to combining the Personal data for cross-context behavioral advertising purposes.

Company acknowledges and understands its obligations under this clause, and will comply with them.

### **14. General**

- 14.1. Any claims brought under this DPA will be subject to the terms and conditions of the Main Agreement, including the exclusions and limitations set forth in the Main Agreement.
- 14.2. In the event of a conflict between the Main Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.
- 14.3. All notices mentioned in this DPA shall be provided by electronic means.
- 14.4. Company may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to Process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.
- 14.5. If Company intends to change this DPA, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will inform Customer (in the Company's portal for customers) at least 10 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.
- 14.6. If the Customer process French health information, Customer should comply with PGSSI, if applicable to it.

By signature, the Parties acknowledge that they have read and understood the terms of this DPA and agree to be legally bound by it:

**CUSTOMER**

Signature \_\_\_\_\_

Print Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

**COMPANY**

Signature \_\_\_\_\_

Print Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

## Exhibit A - SCC

1. If Customer is a Controller – the Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module Two); if Customer is a Processor – the Parties shall be deemed to enter into the Processor to Processor Standard Contractual Clauses (Module Three).
2. This Exhibit A sets out the Parties' agreed interpretation of their respective obligations under Module Two or Module Three of the Standard Contractual Clauses (as applicable).
3. The Parties agree that for the purpose of transfer of Personal Data between the Customer (Data Exporter) and the Company (Data Importer), the following shall apply:
  - 3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.
  - 3.2. In Clause 9, option 2 shall apply.
  - 3.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
  - 3.4. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the laws of the Republic of Ireland. Notwithstanding the forgoing, the UK SCCs shall be governed by the laws of England and Wales.
  - 3.5. In Clause 18(b) the Parties choose the courts of Dublin Ireland, as their choice of forum. Where the UK SCCs apply, the courts of London, England shall have exclusive jurisdiction.
4. To the extent the UK Addendum applies, the following shall apply:
  - 4.1. All the information provided under the Standard Contractual Clauses shall apply to the UK Addendum with the necessary changes per the requirement of the UK Addendum.
  - 4.2. In Table 4 of the UK Addendum, either party may terminate the agreement in accordance with section 19 of the UK Addendum.
  - 4.3. By entering into this Data Protection Agreement, the Parties hereby agree to the formatting changes made to the UK Addendum.

## **ANNEX 1 TO DPA**

This Annex forms an integral part of the DPA.

### **CATEGORIES OF DATA SUBJECTS:**

The Personal Data transferred concern the following categories of Data Subjects:

Individuals whose personal data is on Customer's systems or environments that are monitored by Company's products.

### **CATEGORIES OF PERSONAL DATA:**

Personal Data that is included in the metadata scanned by Varonis software, such as: names, email addresses, IP addresses, information that is included in file and folder names.

For license(s) or service(s) that may require Varonis to process, as part of the Subscriber Data, certain content, then such content will be processed (for example, documents, snippets and prompts).

### **SPECIAL CATEGORIES OR SENSITIVE CATEGORIES OF PERSONAL DATA (AS APPLICABLE):**

No "sensitive" or "special categories" of Personal Data (as these terms are defined under applicable Data

Protection Law) are expected. Customer may, at its sole discretion, opt to share such Personal Data while using the Services.

### **THE FREQUENCY OF THE TRANSFER**

Continuous

### **NATURE OF THE PROCESSING**

Collection, Recording, Organization or structuring, Storage, Adaptation or alteration, Retrieval, Consultation, Disclosure, dissemination or otherwise making available, Analysis.

### **PURPOSE OF THE TRANSFER AND FURTHER PROCESSING**

As defined in the Main Agreement.

### **RETENTION PERIOD**

Personal Data will be retained as detailed in the Main Agreement and the DPA.

## **Annex 2 to DPA**

### **Technical and Organizational Security Measures (Security Schedule)**

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and

organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

More specifically, data Company's security controls shall include:

Domain	Practices
Information Security Policy	<ul style="list-style-type: none"> <li>*Varonis maintain written privacy and security policies, which is consistent in material respects with the requirements of this document and with prevailing industry standards. Such policies support and ensure the confidentiality, integrity, and availability of the Data. Varonis hereby warrants and undertakes that it has and that it will maintain throughout the term of the Agreement a written, comprehensive information security program that complies with applicable laws and information security standards.</li> <li>*Policies are reviewed and approved by management periodically.</li> <li>*Information Security roles and responsibilities are documented and communicated to the relevant personnel.</li> <li>* Varonis designated an Information Security Officer who is operationally responsible for assuring that Varonis complies with security policies, and applicable standards and regulations.</li> </ul>
Access Control	<ul style="list-style-type: none"> <li>*All Varonis system that handles customer data are secured with the described security measures.</li> <li>*Access to customer data is managed through a secure authentication. A formal user registration and de-registration procedures for granting and revoking access to information systems and services is maintained.</li> <li>*Access to customer data is provided on the need to know basis. Access by Varonis personnel who no longer requires access to perform the Services is terminated.</li> <li>*Formal management review of user access rights is performed at regular intervals.</li> <li>*Password policy is enforced to company networks and assets. Password Policy include, and not limited to the settings of password age, length, history, complexity requirements, and account lockout duration.</li> <li>*Session time-out is enforced on company assets.</li> <li>*Administrative and privileged access is restricted to trained and authorized employees of the Data Processor.</li> </ul>
Operations Security	<ul style="list-style-type: none"> <li>*Information backup is conducted regularly, to allow adequate recovery of information in cases of damage to the information or its systems. Backups are protected using industry best practices encryption, and access control.</li> <li>*Periodic restoration tests are performed for scoped data.</li> </ul>

	<p>*Varonis perform periodic technical vulnerability scans on networks, and applications that process, store, or transmit Customer’s Data. Remediation of vulnerabilities is monitored and performed according to a defined procedure.</p> <p>*Malware protection is implemented on Varonis’ assets to avoid malicious software gaining unauthorized access to Customer Data.</p> <p>*Changes to production infrastructure and networks are monitored and controlled through a change management process. Changes are reviewed and approved prior to implementation and recorded after it.</p> <p>*Audit logs recording user activities, exceptions, faults, and information security events are produced, kept, and monitored.</p>
<p><b>Cryptography</b></p>	<p>*Varonis encrypt customer data that is transmitted over public networks, as well as implementing encryption of data at rest.</p> <p>*Strong and non-deprecated versions of encryption algorithms and key lengths are used and monitored.</p> <p>*Keys and secrets are maintained secured. Access to the Keys and secrets is limited to a minimal number of users on a need-to-know basis.</p> <p>*All keys are periodically rotated.</p>
<p><b>Physical and environmental security</b></p>	<p>*Facilities and processing centers are equipped with physical security systems and monitoring as required by security standards (such as ISO/IEC 27001 and/or SOC 2 Type 2), local laws, and regulations.</p> <p>*Varonis limit physical access to its electronic information systems and the facilities in which they are housed, and safeguard those facilities against unauthorized physical access, tampering, and theft.</p> <p>*Clean desk policy is designed to prevent inadvertent disclosure of personal data.</p> <p>*Varonis validates that its cloud service providers maintain physical security policy that is aligned with security industry best-practices, and audited periodically by external third-party auditors (i.e., SOC 2, ISO27001)</p>
<p><b>Communications Security</b></p>	<p>*Varonis applies the principle of least required access for allowed network communications.</p> <p>*All network communications are protected with confidentiality and integrity.</p> <p>*All network communications are monitored for security incidents Remote access to customers’ data is established using a secure, and strong authenticated connection.</p> <p>*Restrictions are in be placed in front of externally exposed applications and endpoints.</p>
<p><b>System Acquisition, Development, and maintenance</b></p>	<p>*Varonis follows formal Secure Software Development cycle.</p> <p>*Rules for the secure software development and systems is established and applied to engineering within the organization.</p> <p>*Testing of security functionality is carried out during the development phases.</p> <p>*Acceptance testing programs and related criteria is established and maintained for systems, upgrades, and new versions.</p>

<p><b>Supplier relationships</b></p>	<ul style="list-style-type: none"> <li>*business arrangements with suppliers, involving their access to Varonis' information, systems and applications shall be based on a formal agreement, consisting of all necessary security and confidentiality relevant to the interaction between Varonis and the suppliers.</li> <li>*Technology service providers undergo a security risk assessment and approved by the CISO department.</li> <li>*Varonis ensure all suppliers which holds customer's data are operating, and providing their service, at a security level that is no less stringent than those outlined in this document.</li> </ul>
<p><b>Information Security Incident Management</b></p>	<ul style="list-style-type: none"> <li>*Varonis shall have an updated policy and procedures to assign responsibilities of Varonis personnel and identification of parties to be notified in case of an information security incident, is in place. Customers can report security incidents related to the scoped services to soc@varonis.com</li> <li>*Varonis is regularly monitoring security events and alerts from production systems to identify abnormal user and system behavior.</li> <li>*Varonis maintains a record of security breaches with sufficient information to allow customers to meet any of its own obligations under relevant data privacy and data security laws and other contractual obligations.</li> </ul>
<p><b>Business continuity management</b></p>	<ul style="list-style-type: none"> <li>*Varonis has a procedure to rebuild cloud environment and recover customer data in case of a disaster causing a destruction before the time it was lost or destroyed.</li> <li>*Infrastructure capacity and applicable third-party services are regularly monitored to minimize service disruption.</li> <li>*Varonis ensures that all dependent cloud service providers have adequate measures for disaster recovery</li> </ul>
<p><b>Compliance</b></p>	<ul style="list-style-type: none"> <li>*Periodically, Varonis will conduct an independent third-party review (such as ISO/IEC 27001 and/or SOC 2 Type 2) of its security policies, and procedures related to the Services provided to Customer. The list of certificates is available in the Trust Center.</li> </ul>
<p><b>Human Resources</b></p>	<ul style="list-style-type: none"> <li>*New hire process is established and includes screening checks and employee's commitment to confidentiality for employees with access to customer data.</li> <li>*Employees undergo periodic security awareness training and are updated on procedures to report security incidents.</li> </ul>
<p><b>Asset Management</b></p>	<ul style="list-style-type: none"> <li>*Asset inventory is maintained and includes ownership and labelling where applicable.</li> <li>*Policy for Acceptable use of assets is developed and implemented in accordance with industry best practices.</li> <li>*Restrictions are in place to prohibit data transfer to removable media.</li> <li>*Varonis ensures that its service providers maintain a secure disposal process when such data is no longer needed.</li> </ul>

Annex 3 to DPA

Name	Product	Purpose of Processing	Location	Scope of processed PII
<b>Microsoft services</b>	All products	<p>Azure - Infrastructure and Platform as a Service (except DatAdvantage Cloud), DevOps App platforms (TFS) - Customer Support management and collaboration, Sentinel - Security information and event management, O365 and Teams - Internal communication</p> <p>Generative AI infrastructure*</p>	<p>Azure cloud – US, EU, UK, Australia, Canada, India, Singapore, United Arab Emirates (except ADO routed through Singapore), Switzerland (except for ADO routed through EU), per customer choice</p> <p>Internal communication – US</p> <p>* Some new Gen AI models are rolled out gradually outside US and EU. Until the rollout, Canada shall be routed to US and the rest – to EU.</p>	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
<b>AWS</b>	<p>DatAdvantage Cloud (DAC)</p> <p>Interceptor</p> <p>Atlas AI</p>	Infrastructure Hosting Service (HIS)	<p>HIS DAC - US, EU, UK, Canada, India, Australia or Singapore, per customer initial choice of cloud locality</p> <p>HIS Interceptor – US</p> <p>HIS Atlas AI – US, EU</p>	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
	All products	SES - Communication application	<p>SES - Per customer initial choice of cloud locality.</p> <p>*Switzerland - routed to EU</p>	
<b>DataDog</b>	DatAdvantage Cloud	Centralized platform for monitoring, visualizing, and alerting on data	<p>US, EU</p> <p>* Canada and India routed to US</p> <p>* The rest are routed to EU</p>	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.

<b>Imperva</b>	All products, except for FedRAMP clients	Web Application Firewall	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
<b>Box</b>	All products, except for FedRAMP clients	Files from Varonis support, advanced services etc. that include logs that may contain PII	Per customer initial choice of cloud locality. * India – routed to Australia * Switzerland – routed to EU * Singapore, United Arab Emirates – routed to Singapore/Japan	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
<b>Salesforce</b>	All products	Support ticket management platform (not including files attached to tickets)	US	Email of client's personnel accessing the system
<b>Okta</b>	All products	Identity Management Solution	US	Email of client's personnel accessing the system
<b>auth0</b>	Atlas AI	Identity Management Solution	US	Email of client's personnel accessing the system
<b>Cloudflare</b>	Atlas AI	Web Application Firewall	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
<b>Torq.IO SOAR</b>	MDDR	MDDR case management platform	US, EU, Japan * Canada routed to US * The rest are routed to EU	Alerts from the Varonis Saas

**Varonis Group Entities**

The following entities are members of the Company Group, and function as sub-processors to provide the services.

Entity Name	Entity Country
<b>Varonis Systems, Inc.</b>	USA
<b>Varonis Systems Ltd.</b>	Israel
<b>Varonis Systems (Ireland) Limited</b>	Ireland

<b>Varonis France SAS</b>	France
<b>Varonis (UK) Limited</b>	UK
<b>Varonis Systems (Deutschland) GmbH</b>	Germany
<b>Varonis Systems (Netherlands) B.V.</b>	The Netherlands and Belgium
<b>Varonis Systems (Luxemburg) S.à r.l.</b>	Luxemburg
<b>Varonis Systems (Poland) sp. Z o.o.</b>	Poland
<b>Varonis Systems Australia Pty Ltd</b>	Australia
<b>Varonis Systems Corp</b>	Canada
<b>Varonis Singapore PTE Ltd.</b>	Singapore
<b>Varonis Systems (India) Private Limited</b>	India
<b>Varonis Systems Japan K.K</b>	Japan

---

## Exhibit D

### Additional Provisions Applicable to Oracle, Inc. Software

1. The software provided by Oracle, Inc. (the "**Oracle Software**") may only be used by the legal entity that executed the Agreement. Notwithstanding the preceding sentence, the Oracle Software may be used by the parent company of such legal entity, and the parent company's majority owned subsidiaries, provided that: (a) each of such entities agrees in writing to be bound by the terms of the Agreement, and (b) the legal entity that executed the Agreement shall be responsible for any breach of the Agreement by any such entity.
2. The Oracle Software may only be used in accordance with the scope of Section 1 of the Agreement and only for your internal business operations. To the extent you are permitted to do so under the Agreement, you may allow agents or contractors (including, without limitation, outsourcers) to use the Oracle Software on your behalf for your internal business operations as described above, subject to the terms of the Agreement. In any such case, you shall be responsible for your agent's, contractor's and outsourcer's, use of the Oracle Software and their compliance with the Agreement.
3. Oracle, Inc. or its licensor retains all ownership and intellectual property rights to the Oracle Software. No title in the Oracle Software is transferred to you or any third party.
4. You may not (a) transfer the Oracle Software except for temporary transfer in the event of computer malfunction; (b) assign, give or transfer the Oracle Software and/or any services related thereto or an interest in them to another individual or entity (in the event you grant a security interest in the Oracle Software and/or any services, the secured party has no right to use or transfer the Oracle Software and/or any services), except to your parent company, and the parent company's majority owned subsidiaries, subject to the limitations provided in Sections 1(a) and 1(b) above; (c) use the Oracle Software for rental, timesharing, subscription service, hosting, or outsourcing; (d) remove or modify any Oracle Software markings or any notice of Oracle's or its licensors' proprietary rights; (e) make the Oracle Software available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted under the Agreement); (f) reverse engineer (unless required by law for interoperability), disassemble or decompile the Oracle Software (the foregoing prohibition includes, but is not limited to, review of data structures or similar materials produced by the Oracle Software) or duplicate the Oracle Software except for a sufficient number of copies of each Oracle Software for your licensed use and one copy of each Oracle Software media.
5. Licensor disclaims, to the extent permitted by applicable law, Oracle's liability for (a) any damages, whether direct, indirect, incidental, special, punitive or consequential, and (b) any loss of profits, revenue, data or data use, arising from the use of the programs.
6. Upon the termination of the Agreement, you shall discontinue use and destroy or return to Licensor all copies of the Oracle Software and related documentation.
7. You may not publish any results of benchmark tests run on the Oracle Software.
8. You shall comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Oracle Software, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws.
9. The Oracle Software is subject to a restricted license and can only be used in conjunction with the Software; You are not allowed to modify the Oracle Software.
10. Licensor may audit your use of the Oracle Software. You will provide reasonable assistance and access to information in the course of such audit. Licensor may report the audit results to Oracle or assign its right to audit your use of the Oracle Software to Oracle. Licensor and Oracle shall not be responsible for any costs incurred by you in cooperating with the audit. Some Oracle Software may include source code that Oracle may provide as part of its standard shipment of such programs, which source code shall be governed by the terms of the Agreement.
11. Third party technology that may be appropriate or necessary for use with some Oracle Software is specified in the applicable documentation or shall otherwise be notified by Licensor. Such third party

technology is licensed to you only for use with the Oracle Software under the terms of the third party license agreement specified in the applicable documentation or as otherwise notified by Licensor and not under the terms of the Agreement.

**\*\*\*\*\*In the event you are a governmental or public sector entity, the below Exhibit A-1 shall apply to you instead of Exhibit A\*\*\*\*\***

#### Exhibit A-1

##### Additional Provisions Applicable to Oracle, Inc. Software for Government Entity

1. The software provided by Oracle, Inc. (the "**Oracle Software**") may only be used by the legal entity that executed the Agreement. Notwithstanding the preceding sentence, the Oracle Software may be used by the parent company of such legal entity, and the parent company's majority owned subsidiaries, provided that: (a) each of such entities agrees in writing to be bound by the terms of the Agreement, and (b) the legal entity that executed the Agreement shall be responsible for any breach of the Agreement by any such entity.
2. The Oracle Software may only be used in accordance with the scope of Section 1 of the Agreement, including the license definitions and rules set forth in the Oracle Software documentation, and only for your internal business operations. To the extent you are permitted to do so under the Agreement, you may allow agents or contractors (including, without limitation, outsourcers) to use the Oracle Software on your behalf for your internal business operations as described above, subject to the terms of the Agreement. In any such case, you shall be responsible for your agent's, contractor's and outsourcer's use of the Oracle Software and their compliance with the Agreement. Oracle's license definitions and rules are subject to change and are available at <http://partner.oracle.com> (log in, select Membership / Agreements & Policies).
3. Ancillary programs may only be used for the purposes of installing or operating the Oracle Software with which the ancillary programs are delivered. For the purpose hereof, "ancillary programs" are third party materials specified in the Oracle Software documentation.
4. Oracle, Inc. or its licensor retains all ownership and intellectual property rights to the Oracle Software. No title in the Oracle Software is transferred to you or any third party.
5. The Oracle Software is subject to a restricted license and can only be used in conjunction with the Software.
6. Third party technology that may be appropriate or necessary for use with some Oracle Software as specified in the applicable documentation or as otherwise notified by Licensor and such third party technology is licensed to you only for use with the Oracle Software under the terms of the third party license agreement specified in the applicable documentation or as otherwise notified by Licensor and not under the terms of the Agreement.
7. The Oracle Software is not specifically designed, manufactured or intended for use as parts, components or assemblies for the planning, construction, maintenance or operation of a nuclear facility and may not be used for these purposes.
8. You may not (a) transfer the Oracle Software except for temporary transfer in the event of computer malfunction; (b) assign, give or transfer the Oracle Software and/or any services related thereto or an interest in them to another individual or entity (in the event you grant a security interest in the Oracle Software and/or any services, the secured party has no right to use or transfer the Oracle Software and/or any services and if you decide to finance your acquisition of the Oracle Software you must follow Oracle's policies regarding financing which are available at <http://oracle.com/contracts>) except to your parent company, and the parent company's majority owned subsidiaries, subject to the limitations provided in Sections 1(a) and 1(b) above; (c) use the Oracle Software for rental, timesharing, subscription service, hosting, or outsourcing; (d) remove or modify any Oracle Software markings or any notice of Oracle's or its licensors' proprietary rights; (e) make the Oracle Software available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted under the Agreement); (f) reverse engineer (unless required by law for interoperability), disassemble or

decompile the Oracle Software (the foregoing prohibition includes, but is not limited to, review of data structures or similar materials produced by the Oracle Software) or duplicate the Oracle Software except for a sufficient number of copies of each Oracle Software for your licensed use and one copy of each Oracle Software media.

9. Any additional programs that Oracle may include with the Oracle Software ordered may be used by you only for trial, non-production purposes only. You may not use such additional programs included with an order to provide training or attend training provided by Licensor or a third party on the content and/or functionality of such programs. You have 30 days from the delivery date to evaluate the additional programs, subject to the terms of the Agreement. If you decide to use any additional programs after the 30 day trial period, you must obtain a license for such programs from Licensor. If you decide not to obtain a license for the additional programs after the 30 day trial period, you will cease using and will delete any such programs from your computer systems. Additional programs included with an order are provided "as is," and Oracle does not provide technical support or offer any warranties for these programs.

10. Technical support, if ordered from Oracle, is provided under Oracle's technical support policies in effect at the time the services are provided and that Oracle's technical support policies can be accessed at <http://oracle.com/contracts>. You acknowledge that Oracle's technical support policies are incorporated into the Agreement by reference. If you decide not to purchase technical support on the date hereof, then you will be required to pay reinstatement fees to Oracle in accordance with Oracle's current technical support policies if you decide to purchase support at a later date.

11. Any third party firms retained by you to provide computer consulting services are independent of Oracle and are not Oracle's agents, and Oracle is not liable for nor bound by any acts of any such third party firm.

12. Some Oracle Software may include source code that Oracle may provide as part of its standard shipment of such programs, which source code shall be governed by the terms of the Agreement.

13. Licensor disclaims, to the extent permitted by applicable law, Oracle's liability for (a) any damages, whether direct, indirect, incidental, special, punitive or consequential, and (b) any loss of profits, revenue, data or data use, arising from the use of the programs.

14. Upon the termination of the Agreement, you shall discontinue use and destroy or return to Licensor all copies of the Oracle Software and related documentation.

15. You may not publish any results of benchmark tests run on the Oracle Software.

16. You shall comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Oracle Software, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws.

17. Licensor may audit your use of the Oracle Software. You will provide reasonable assistance and access to information in the course of such audit. Licensor may report the audit results to Oracle or assign its right to audit your use of the Oracle Software to Oracle. Licensor and Oracle shall not be responsible for any costs incurred by you in cooperating with the audit.

18. You hereby confirm that you have not relied on the future availability of any hardware, programs or updates in entering into the Agreement; however, (a) if you order technical support from Oracle, the preceding sentence does not relieve Oracle of its obligation to provide updates under such order, if-and-when available, in accordance with Oracle's then current technical support policies, and (b) the preceding sentence does not change the rights granted to you for any Oracle Software licensed under the Agreement, per the terms of the Agreement.

19. You hereby confirm that the Uniform Computer Information Transactions Act does not apply to this Exhibit A-1.

20. This Exhibit A-1 is subject to change at Oracle's discretion upon 30 days' notice.