

APPENDIX G:

PING MASTER SERVICE AGREEMENT

1. General.

1.1 Provision of Service. Ping Identity shall make the Service available to Customer during the subscription term specified in the applicable Order Form(s) and grants to Customer a limited, non-exclusive, non-sublicenseable, non-transferable right to access and use the Service, solely for Customer's business use, all in accordance with this Agreement, the applicable Order Form(s) and the Documentation.

1.2 Software License Grant. Ping Identity hereby grants Customer, during the subscription term specified in the applicable Order Form(s), a limited, non-exclusive, non-sublicenseable, non-transferable license to install the Software, in machine-readable form only, and to use the Software solely for Customer's business use, all in accordance with this Agreement, any applicable Order Form(s) and the Documentation.

1.3 Delivery and Installation of the Software. The Software will be delivered to Customer by electronic download. Customer will be solely responsible for installing any Software as permitted under this Agreement unless otherwise set forth in an Order Form. All Software will be deemed accepted upon delivery unless otherwise set forth in an Order Form.

1.4 Support for Products. Subject to Customer's payment of all applicable Fees, Customer shall be entitled to receive support for the Products as set forth in Exhibit A ("Support Services"). Ping Identity is not obligated under the terms of this Agreement to provide any customer service or Support Services to any User other than Customer's administrators; such responsibility (if any) shall remain with Customer.

2. Use Guidelines.

2.1 Restrictions. Customer shall use the Products solely for its own business purposes in accordance with this Agreement and any related Order Form. Except as expressly permitted by this Agreement, Customer shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, operate as a service bureau or managed service, or otherwise commercially exploit or make the Products available to any third party; (ii) modify, adapt, alter, translate or create derivative works of the Products or Deliverables; (iii) reverse engineer, decompile or disassemble the Products or Deliverables (or otherwise attempt to derive the source code or underlying ideas or algorithms of the Software); (iv) take any action that would cause the Products or Deliverables (including any license key) to be placed in the public domain; (v) remove, alter, or obscure any proprietary notices of Ping Identity, its licensors or supplier included in the Products or Deliverables; (vi) use the Products or Deliverables to send or store Malicious Code or infringing, obscene, threatening, harmful, illegal, fraudulent, abusive, defamatory, libelous, or otherwise unlawful or tortious material or spam intended to damage any system or data; (vii) interfere with or disrupt the integrity or performance of the Service or the data contained therein or other equipment or networks connected to the Service, or disobey any requirements made known to Customer; (viii) attempt to gain unauthorized access to the Service or its related systems or networks or collect, transmit or use information, or distribute software which covertly gathers or transmits information about a user; (ix) circumvent, disable, or interfere with security-related features of the Products or Deliverables, or features that enforce limitations on use of the Products or Deliverables; (x) access the Products or Deliverables for the purpose of building a competitive product or service or copying its features or user interface; (xi) send or store any personal health information (unless Customer and Ping Identity execute an Order Form for the relevant Identity Licenses that includes or references the relevant Business Associate Agreement), credit card data, personal financial data or other sensitive data (as defined under applicable data privacy laws) that may be, without limitation, subject to the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, or the Payment Card Industry Data Security Standards; or (xii) conduct any High-Risk Activities, defined as uses such as the operation of nuclear facilities, a air traffic control or other transportation systems, or life support systems, where the use or failure of the Service could lead to death, personal injury, or environmental damage; or (xiii) conduct that is likely to breach any applicable laws, codes or regulations applicable to the parties or others. Customer acknowledges that certain Services have rate limiting in effect for the protection of the Service, and that add-on upgrades may be available for purchase if additional throughput is needed.

2.2 Customer Responsibilities. Customer shall: (i) have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Customer Data submitted by it and its Users to the Service; (ii) identify and authenticate all Users and approve and control access by such Users of the Products; (iii) maintain the confidentiality of usernames, passwords and account information and notify Ping Identity promptly of any unauthorized access or use; and (iv) have sole responsibility for all activities that occur under its and its Users' usernames, passwords or accounts as a result of Customer's or Customer's Users' access to the Products and Documentation. Customer is responsible for all actions and omissions of its Users as if they were those of Customer hereunder. If Customer becomes aware of any violation of Customer's obligations under this Agreement by any User, Customer will promptly notify Ping Identity and work with Ping Identity to promptly terminate access of any such User to the Products. Ping Identity reserves the right but not the obligation to remove, or request that Customer remove, any Customer Data from the Service that is reasonably believed to be unlawful or harmful to the Service or if a third party brings or threatens legal action regarding such data. Customer shall comply with any applicable Ping Identity security guidelines and procedures as set forth in the Documentation.

2.3 Compliance with Laws. Each Party shall comply with all applicable local, state, national and foreign laws applicable to such Party in connection with this Agreement. Customer shall obtain any authorizations, consents or rights from Users and Third-Party Providers (defined later herein) that are required, and provide any necessary notifications, in each case for the transmission of Personal Information to Ping Identity and other third parties in connection with the Products and the related use and processing by such persons, including as may be necessary under any data protection laws and regulations. Customer shall not provide any Personal Information to Ping Identity that may not be processed by Ping Identity as set forth herein. If required, Customer will include in its applicable privacy policies and/or terms of use any necessary disclosures regarding data collection and usage (including with respect to transfer to third parties) in connection with its use of the Products. Customer agrees (i) to comply with all applicable export control and sanctions laws, including those of the United States, in connection with any export, re-export or transfer of the Products and (ii) to not provide any Product for end use by or to end users in Belarus, Cuba, Iran, North Korea, Russia, Sudan, Syria, Venezuela, the Crimea region of Ukraine, the so-called “Donetsk People’s Republic,” or the so-called “Luhansk People’s Republic,” (or any other country that becomes subject to comprehensive sanctions by the United States), or to any person or entity that is otherwise subject to restrictions, without prior written consent of Ping Identity.

2.4 Suspension of Service for Critical Cause. Ping Identity reserves the right to suspend or terminate the Service or any portion thereof provided to Customer if: (i) suspension of the Service is necessary to comply with the law; or (ii) there are material security or vulnerability risks to the Service, excessive fraudulent or abusive acts or omissions, or Customer’s use of the Service is in violation of this Agreement. Ping Identity will give advance notice of the suspension, to the extent it is able without causing undue harm or risk. Any such suspension will be limited in scope to only the affected Products; and Ping Identity will exhaust commercially reasonable options with the Customer other than suspension prior to initiating any suspension in connection therewith. Ping Identity will restore access to the Service in a prompt manner after the underlying cause is mitigated. No credit or remedy under any service level agreement for interruption of service is available if such interruption of service was affected under this clause.

3. Fees & Payment.

3.1 Direct Purchases from Ping Identity.

(a) Fees. For direct purchases with Ping Identity, Customer shall pay all fees specified in any Order Forms hereunder (the “Fees”). Except as otherwise specified herein or in an Order Form, stated Fees are based on the scope of the Product subscriptions purchased and not actual usage, payment obligations are non-cancelable, Fees paid are non-refundable, and all Fees are quoted and payable in currency stated on the Order Form. Customer agrees that its purchase of the Products is neither contingent upon the delivery of any future functionality or features, nor is it dependent upon any oral or written public comments made by Ping Identity with respect to future functionality or features.

(b) Usage Reconciliation. The Parties shall meet on a regular basis to review Customer’s usage of the Products against the applicable entitlements set forth in the Order Form.

(c) Invoicing & Payment Terms. All Fees will be invoiced in advance and in accordance with the relevant Order Form. Unless otherwise stated in an Order Form, charges are due net thirty (30) days from the date of the invoice. Customer is responsible for maintaining complete and accurate billing and contact information.

(d) Late Payment. Timeliness of payment and any interest to be paid to Ping Identity for late payment shall be governed by Article 11-A of the State Finance Law to the extent required by law.

(e) Taxes. Customer is responsible for paying or self-assessing all applicable direct or indirect local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added, sales, use or withholding taxes (collectively, “Taxes”) associated with its purchases hereunder, above and beyond the Fees, excluding taxes based on Ping Identity’s net income or property, unless Customer provides Ping Identity with a valid tax exemption certificate authorized by the appropriate taxing authority. To the extent that any amounts payable by you are subject to withholding taxes, the amount payable shall be grossed up such that the amount paid to Ping Identity net of withholding taxes equals the amount invoiced by Ping Identity. Unless otherwise stated, all prices set forth on an Order Form are exclusive of Taxes.

3.2 Reseller and/or Marketplace Purchases.

(a) If Customer purchases Products, Support Services, or Professional Services through a Reseller and/or Marketplace, this Agreement will govern Customer’s use of such Products, Support Services, or Professional Services, but not the payment obligations. In such case, Customer’s payment obligations for the Products, Support Services, or Professional Services will be as agreed directly with the Reseller or as arranged through the Marketplace, as applicable, and not Ping Identity. Customer warrants that it will timely pay to Reseller or the Marketplace all amounts related to this Agreement. Notwithstanding the foregoing, any variable fees or

reimbursements, such as SMS fees, may be required to be remitted directly to Ping Identity in lieu of a Marketplace in the event that there is not a reasonable mechanism to invoice such fees through the Marketplace. Customer expressly waives and agrees not to exercise any right it may have to downgrade a subscription, terminate a purchase of Products, Support Services, or Professional Services for its convenience, or otherwise cancel an order under any applicable Reseller or Marketplace terms and conditions, except as expressly permitted by this Agreement. Any disputes related to the payment obligations shall be handled directly between Customer and the Reseller or Marketplace, as applicable. Any listing on a Marketplace is simply an offer to make purchases of Products and Professional Services subject to this Agreement, and no terms included in such listing are incorporated herein.

(b) If a Reseller notifies Ping Identity that the Reseller is entitled to, and seeks to, terminate or suspend any Ping Identity Offerings and/or Other Services purchased by Customer through the Reseller pursuant to the agreement between Customer and Reseller, Ping Identity may suspend or terminate the Ping Identity Products, Support Services, or Professional Services identified by the Reseller. Subsequently, if Partner notifies Ping Identity that Customer is entitled to reinstatement of any suspended Products and/or other services pursuant to the Partner Agreement, and Customer is otherwise in compliance with the terms of this Agreement, Ping Identity shall reinstate the suspended Products, Support Services, or Professional Services as soon as reasonably practicable. Ping Identity shall not be liable to Customer or to any third party for any liabilities, claims, or expenses arising from or relating to any suspension or termination or reinstatement of Products, Support Services, or Professional Services in accordance with this section.

3.3 Audit of Software Usage. Upon Ping Identity's request, no more than once every twelve (12) months, Customer shall provide a certification or representation in writing, executed by one of its duly authorized executive officers, that Customer is using the Software in accordance with the terms and conditions of this Agreement.

4. Confidentiality.

4.1 Confidentiality. The Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, except with the Disclosing Party's prior written permission. The Receiving Party may disclose Confidential Information to its Affiliates, service providers and subcontractors on a need-to-know basis, and such Affiliates, service providers and subcontractors may use such Confidential Information, in each case only for the purposes of fulfilling Receiving Party's obligations under this Agreement. The Receiving Party shall be liable to the Disclosing Party for all actions and omissions of its Affiliates, service providers and subcontractors with respect to such information as if such actions and omissions were those of the Receiving Party hereunder. Confidential Information shall not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (iii) was independently developed by the Receiving Party without breach of any obligation owed to the Disclosing Party; or (iv) is received from a third party without breach of any obligation owed to the Disclosing Party.

4.2 Protection. The Receiving Party agrees to protect the confidentiality of the Confidential Information of the Disclosing Party in the same manner that it protects the confidentiality of its own proprietary and confidential information of like kind (but in no event using less than reasonable care), and promptly notify the Disclosing Party upon discovery of any unauthorized access or acquisition of Confidential Information and reasonably cooperate with the Disclosing Party's efforts to prevent, investigate and remediate the breach of confidentiality.

4.3 Compelled Disclosure. If the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. In the event that the Receiving Party is nevertheless compelled to make such a disclosure, it shall disclose the minimum necessary Confidential Information to comply with such request.

4.4 Remedies. If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of confidentiality protections hereunder, the Disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the Parties that any other available remedies are inadequate.

4.5 Retention of Confidential Information. Upon a Party's written request, the other Party will erase, delete or destroy all copies of Confidential Information of the other Party whether or not modified or merged into other materials, and certify in writing to the other Party that such Party has fully complied with these requirements. A Party may retain copies of Confidential Information that are required to be retained by law or pursuant to such Party's reasonable document retention policies, or copies that are incapable of being destroyed because it would be unduly burdensome or cost prohibitive, provided that all such copies remain subject to the restrictions herein for so long as they are retained.

5. Customer Data and Security.

5.1 Customer Data. Ping Identity shall not provide the Customer Data to any third parties except as necessary to operate the Service. Customer hereby represents and warrants to Ping Identity that the Customer Data is free of all viruses, Trojan horses, and comparable elements which could harm the systems or software used by Ping Identity or its subcontractors to provide the Service. Customer agrees that it has collected and shall maintain and handle all Customer Data and Personal Information in compliance with applicable law.

5.2 Information Security, Audits and Security Assessments. Ping Identity will implement and maintain reasonable and appropriate technical, organizational, administrative and physical security measures designed to protect against unauthorized access to or use of Customer Data. During the Subscription Term, Ping Identity shall comply with Ping Identity's security documentation attached hereto as Exhibit B and Exhibit C.

5.3 Business Continuity/Disaster Recovery. During the term of this Agreement, Ping Identity will maintain and comply with its then-current Business Continuity and Disaster Recovery Plans. Ping Identity will test such plans at least annually. Upon written request, Ping Identity will provide (i) a copy of the table of contents to such plan, and (ii) a summary of its annual testing results.

5.4 Data Privacy Addendum. The Data Privacy Addendum set forth in Exhibit D (the "DPA") is incorporated by reference into this Agreement.

5.5 Retrieval of Customer Data. Customer shall have the ability to access Customer Data at any time during a subscription term. Thirty (30) days after the effective date of termination, Ping Identity shall have no obligation to maintain or provide any Customer Data and Ping Identity may delete any Customer Data, environment, organization or any other Customer information or materials related to the Service or provided to Ping Identity by Customer in connection with the Service unless prohibited by applicable law. During such thirty (30) day period, Customer shall have the option to retrieve the Customer Data from the Service, except for data that, if accessed or exported, could compromise the security or integrity of the Service, including but not limited to password hashes or other sensitive system-level data.

5.6 Data Residency. With respect to the Service, if Customer selects data center(s) in the United States, Customer Data shall be stored solely in the United States. Notwithstanding the foregoing, Customer Data may be accessed by personnel of Ping Identity located at any of the locations identified in the DPA, solely to the extent necessary for purposes of maintenance, technical support, security, or operational continuity, and subject at all times to the confidentiality, data protection, and security obligations set forth herein.

6. Proprietary Rights.

6.1 Reservation of Rights. Subject to the limited rights expressly granted hereunder, Ping Identity reserves all rights, title and interest in and to the Products (and any enhancements, modifications, or derivative works thereof, or other software development and works performed by Ping Identity), including all related Intellectual Property Rights. As between Ping Identity and Customer, Customer owns all rights, title and interest in and to all Customer Data. No rights are granted to Customer hereunder other than as expressly set forth herein.

6.2 Suggestions. Ping Identity shall have a royalty-free, worldwide, transferable, sublicenseable, irrevocable, perpetual license to use or incorporate into its products and services any suggestions, enhancement requests, recommendations or other feedback provided by Customer or its Users relating to the operation of the Products.

6.3 Usage Data. Ping Identity owns any data derived from the operation of the Products that has been aggregated and de-identified so that results are non-personally identifiable with respect to Customer or any User, and nothing herein will prohibit Ping Identity from using such data in the operation of Ping Identity's business.

7. Professional Services.

7.1 Ping Responsibilities. Ping Identity will perform Professional Services and deliver to Customer all items set forth in an Order Form or SOW executed pursuant to this Agreement.

7.2 Customer Responsibilities. Customer will make available in a timely manner for Ping Identity's use, at no charge to Ping Identity, all technical data, files, documentation, test data, sample output or other information, resources and personnel required by Ping Identity for the performance of the Professional Services under this Agreement and the SOW(s). Customer will be responsible for, and assumes the risk of, any issues or problems resulting from: (i) the content, accuracy, completeness or consistency of all Customer

computer facilities, programs, files, documentation, test data, sample output or other information and resources; and (ii) the competence of the personnel supplied by Customer.

7.3 Background Checks and Screening. Ping Identity performs background checks on each of its employees, including criminal background checks, prior to their commencement of employment with Ping Identity and in accordance with applicable law. Ping Identity will not assign any personnel to perform Professional Services that do not pass such background checks to Ping Identity's reasonable satisfaction. Ping Identity also requires any relevant subcontractor to perform background checks on their own personnel. If Customer has additional specific screening requirements, Customer shall be permitted to request that persons performing Professional Services hereunder undergo additional reasonable screening requirements, to be performed by Customer at its own expense and Customer will be responsible for obtaining the consent of all applicable personnel. Customer's sole remedy for any personnel that refuse to undertake reasonable additional screening requirements shall be the replacement of the personnel performing such Professional Services at no additional costs to Ping Identity.

8. Warranties & Disclaimers.

8.1 Warranties. Each Party represents that it has the legal power to enter into this Agreement. Each Party further represents that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against such Party in accordance with its terms; (b) no authorization or approval from any other person is required in connection with such Party's execution, delivery, or performance of this Agreement; and (c) the execution, delivery, and performance of this Agreement does not violate the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.

8.2 Performance Warranty for Products. For a period of ninety (90) days after the date of delivery of the Software and for the duration of a subscription to the Service (in each case, the "**Warranty Period**"), Ping Identity warrants that the Products, when used as permitted by Ping Identity and in accordance with the Documentation, will operate substantially as described in the Documentation. Ping Identity will, at its own expense and as its sole obligation and Customer's exclusive remedy for any breach of this warranty, use commercially reasonable efforts to (i) correct any material reproducible error that Customer reports to Ping Identity in writing during the Warranty Period, or (ii) replace the defective Product. If Ping Identity, in its sole discretion, may not achieve either (i) or (ii) as a remedy for breach of this warranty, Ping Identity agrees to accept return of the Product, terminate the subscription to the defective Product and refund Customer all unused, prepaid Fees with respect to the defective Product.

8.3 Professional Services Warranty. Ping Identity warrants that it will provide the Professional Services using reasonable care and skill, and in a manner consistent with industry standards applicable to the provision thereof. As Customer's exclusive remedy for a breach of the foregoing warranty, if Customer notifies Ping Identity in writing within ten (10) days of completion of the applicable Professional Services, Ping Identity will, at its own expense and as its sole obligation, reperform the Professional Services. This warranty shall not apply with respect to (a) modification of the Deliverables other than by Ping Identity; (b) a abuse, misuse or improper installation of the Deliverable; or (c) a change to Customer's computing environment that would affect the specific Deliverable.

8.4 Disclaimer. THE PRODUCTS AND PROFESSIONAL SERVICES ARE PROVIDED "AS IS" AND, EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH HEREIN, PING IDENTITY AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. PING IDENTITY DOES NOT WARRANT THAT THE PROFESSIONAL SERVICES OR THE FUNCTIONS CONTAINED IN THE PRODUCTS WILL MEET CUSTOMER'S REQUIREMENTS, OR THAT THE OPERATION AND RESULTS OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE PRODUCTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY PING IDENTITY OR ITS AUTHORIZED REPRESENTATIVES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF ANY WARRANTY HEREIN. PING IDENTITY WARRANTS THAT IT OWNS OR HAS THE RIGHT TO LICENSE AND DISTRIBUTE ALL THIRD-PARTY SERVICES PROVIDED UNDER THIS AGREEMENT.

9. Indemnification.

9.1 Indemnification by Ping Identity. Ping Identity will defend at its own expense any action against Customer brought by a third party alleging that the Products, in each case, as delivered, infringe any patents, copyrights or misappropriate any trade secrets, in each case, of a third party, and Ping Identity will indemnify and hold Customer harmless without limitation against those costs and damages finally awarded against Customer in any such action or those costs and damages agreed to in a monetary settlement of such action. If the Products become, or in Ping Identity's opinion are likely to become, the subject of an infringement claim, Ping Identity may, at its option and expense, either: (i) procure for Customer the right to continue using the Products; (ii) replace or modify the Products so that they become non-infringing; or (iii) terminate the subscription to the infringing Products and refund Customer any unused, prepaid Fees for the infringing Products covering the remainder of the subscription term after the date of termination. Notwithstanding the foregoing, Ping Identity will have no obligation or liability under this Section 9.1 or otherwise with respect to any infringement or misappropriation

claim based upon: (a) any use of the Products not in accordance with this Agreement; (b) any use of the Products in combination with products, equipment, software, or data not supplied or approved in writing by Ping Identity if such infringement would have been avoided but for the combination with other products, equipment, software or data; (c) any use of a prior release of the Software after a more current release has been made available to Customer; or (d) any modification of the Products by any person other than Ping Identity. THIS SECTION 9.1 STATES PING IDENTITY'S ENTIRE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY FOR ANY CLAIMS OF INFRINGEMENT OR MISAPPROPRIATION.

9.2 Indemnification Conditions. "Indemnification Conditions" means the following conditions, which Customer must comply with to be entitled to the defense and indemnification obligations of Ping Identity under this Agreement. The Customer must (i) notify Ping Identity promptly in writing of such claim or allegation, setting forth in reasonable detail the facts and circumstances surrounding the claim, provided that Customer's failure to promptly notify shall only relieve Ping Identity's indemnification obligations to the extent Ping Identity was prejudiced by such failure; (ii) give Ping Identity sole control of the defense thereof and any related settlement negotiations, provided that Customer may participate in its defense at its own cost and expense, and shall not make any admission of liability or take any other action that limits the ability of Ping Identity to defend or settle the claim; and (iii) cooperate and, at the Ping Identity's request and expense, assisting in such defense or settlement.

10. Limitation of Liability.

10.1 Limitation of Liability. PING IDENTITY'S CUMULATIVE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) SHALL NOT EXCEED THREE TIMES THE TOTAL AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER TO PING IDENTITY OR TO A RESELLER OF PING IDENTITY HEREUNDER FOR THE PRODUCT OR PROFESSIONAL SERVICE GIVING RISE TO THE LIABILITY IN THE 12 MONTHS PRECEDING THE INCIDENT, OR THE CUSTOMER'S ACTUAL DAMAGES, WHICHEVER IS LOWER. THE FOREGOING SHALL NOT APPLY TO THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 9, TO CUSTOMER'S PAYMENT OBLIGATIONS UNDER SECTION 3, OR PING IDENTITY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT. Notwithstanding the foregoing, Ping Identity remains liable, without monetary limitation, for direct damages for personal injury, death or damage to real property or tangible personal property or intellectual property attributable to the negligence or other tort of Ping Identity, its officers, employees or agents. For clarity, any claims relating to third-party intellectual property infringement shall be governed exclusively by Section 9.1.

10.2 Exclusion of Consequential and Related Damages. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR (i) ERROR OR INTERRUPTION OF USE, LOSS OR INACCURACY OR CORRUPTION OF DATA, (ii) COST OF COVER, (iii) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF REVENUES AND LOSS OF PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING EXCLUSIONS WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

11. Term & Termination.

11.1 Term of Agreement. This Agreement commences on the Effective Date and continues for as long as the subscription term set forth in any related Order Form (and any subsequent Order Forms) or as otherwise agreed to by Ping Identity in writing, unless earlier terminated as set forth herein.

11.2 Termination for Cause. Either Party may terminate this Agreement for cause: (i) upon thirty (30) days written notice of a material breach of this Agreement by the other Party if such breach remains uncured at the expiration of such period; or (ii) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

11.3 Effects of Termination. Upon expiration or termination of this Agreement all rights to use the Products (including all licensed rights for the Software) granted in this Agreement will immediately cease to exist and Customer must promptly discontinue all use of the Products.

11.4 Outstanding Fees. Termination does not relieve Customer of the obligation to pay any Fees accrued or payable to Ping Identity prior to the effective date of termination. Upon any termination for cause by Customer, Ping Identity will refund Customer any unused, prepaid Fees covering the remainder of the subscription term after the date of termination. Termination for Customer's material uncured breach does not relieve Customer of any obligation to pay Fees that would have been payable but for such termination.

11.5 Surviving Provisions. Any provisions that are by their nature intended to survive termination of this Agreement will continue to survive following termination.

12. General Provisions.

12.1 Relationship of the Parties. The Parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, a agency, fiduciary or employment relationship between the Parties. Neither Party will have the power to bind the other or incur obligations on the other Party's behalf without the other Party's prior written consent.

12.2 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

12.3 Notices. All notices under this Agreement shall be in writing and may be sent by electronic mail. Notices shall be deemed to have been given upon the second business day after sending by email. Notices to Ping Identity shall be sent to legalnotice@pingidentity.com. Notices to Customer, unless otherwise indicated by Customer, may be sent to the individual that executed this Agreement on behalf of Customer and/or an Administrator by email, or at the address listed at the beginning of this Agreement.

12.4 Waiver and Cumulative Remedies. Failure or delay by either Party to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision of this Agreement. Other than as expressly stated herein, the rights and remedies provided herein are in addition to, and not exclusive of, any other rights and remedies of a Party at law or in equity.

12.5 Intentionally Omitted.

12.6 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in force and effect.

12.7 Third-Party Services. The Products may be used by Customer in connection with services or applications that interoperate with the Products that are provided by Customer or a third party ("**Third-Party Services**"). Third Party-Services are not Products nor provided by Ping Identity, and their use by Customer is subject to Customer's agreement with their applicable providers ("**Third-Party Providers**"). Ping Identity does not guarantee that the Products will interoperate with any particular Third-Party Service, and Ping Identity's support obligations shall not extend to any Third-Party Services.

12.8 Open Source Software. Certain items of software embedded within the Products are subject to "open source" or "free software" licenses ("**Open Source Software**"). Some of the Open Source Software is owned by third parties. Nothing in this document limits Customer's rights or obligations under the terms and conditions of any applicable end user license for the Open Source Software. Ping Identity warrants that it owns or has the right to license and distribute all open source software provided under this Agreement. In no event do any authors of any Open Source Software provide any warranties with respect to such Open Source Software and such authors disclaim liability of any kind for any use of the Open Source Software. The terms of the licenses for the Open Source Software shall not impose any additional restrictions on your use of the Products as permitted by this Agreement or negate or amend any of our responsibilities with respect to the Products.

12.9 Trial Products. If Customer uses a Product or functionality that Ping Identity makes available to Customer to try at Customer's option for purposes of evaluation or which is designated as "beta," "trial," "pre-GA," "pilot," "preview," "early access," "evaluation," "proof of concept (POC)," or by a similar designation or made available to Customer at no cost ("**Trial Product**"), then the applicable provisions of this Agreement will govern that Trial Product (unless otherwise agreed), and Ping Identity will make such Trial Product available to Customer on a trial basis until the earlier of (a) the end of the trial period for which Customer agreed to use such Trial Product, (b) the start date of any subscription purchased by Customer for such Product, or (c) termination of the Trial Product by Ping Identity in its sole discretion. A trial period may be extended upon mutual agreement by Ping Identity and Customer. Customer is not permitted to use Trial Products in connection with Personal Information. Customer represents and warrants that it will only use test or mock data with Trial Products. Ping Identity warrants that it owns or has the right to license and distribute all Trial Products provided under this Agreement. Notwithstanding anything to the contrary in this Agreement, a Trial Product is provided "AS IS." PING IDENTITY MAKES NO OTHER REPRESENTATIONS OR WARRANTIES AND SHALL HAVE NO INDEMNIFICATION OBLIGATIONS WITH RESPECT TO A TRIAL PRODUCT OTHER THAN AS SET FORTH IN SECTION 9.1 OF THIS AGREEMENT. PING IDENTITY SHALL NOT HAVE ANY LIABILITY FOR CUSTOMER'S USE OF THE TRIAL PRODUCTS UNDER THIS AGREEMENT UNDER ANY THEORY OF LIABILITY (NOWITHSTANDING ANY LIMITATION OF LIABILITY CONTAINED ELSEWHERE HEREIN), UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE PING IDENTITY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING

TO A TRIAL PRODUCT IS \$1,000. ANY DATA AND CONFIGURATIONS ENTERED INTO CUSTOMER'S TRIAL PRODUCT ACCOUNT MAY BE PERMANENTLY LOST UPON TERMINATION OF THE TRIAL PRODUCT TERM.

12.10 NON-ASSIGNMENT CLAUSE. In accordance with Section 138 of the State Finance Law, this contract may not be assigned by Ping Identity or its right, title or interest therein assigned, transferred, conveyed, sublet or otherwise disposed of without the State's previous written consent, and attempts to do so are null and void. Notwithstanding the foregoing, such prior written consent of an assignment of a contract let pursuant to Article XI of the State Finance Law may be waived at the discretion of the contracting agency and with the concurrence of the State Comptroller where the original contract was subject to the State Comptroller's approval, where the assignment is due to a reorganization, merger or consolidation of Ping Identity's business entity or enterprise. The State retains its right to approve an assignment and to require that Ping Identity demonstrate its responsibility to do business with the State. Ping Identity may, however, assign its right to receive payments without the State's prior written consent unless this contract concerns Certificates of Participation pursuant to Article 5-A of the State Finance Law.

12.11 Applicable Law and Venue; Jurisdiction. Disputes involving this contract, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily authorized), but must, instead, be heard in a court of competent jurisdiction of the State of New York. **Governing Language.** The governing language for this Agreement and for negotiation and resolution of any disputes related to this Agreement is the English language. Each Party waives any right it may have under any law in any state or country to have the Agreement written in any language other than English.

12.12 Force Majeure. If the performance of this Agreement or any obligation hereunder (other than obligations of payment) is prevented or restricted by reasons beyond the reasonable control of a Party including but not limited to computer related attacks, hacking, war, sanctions, riots, any law or any action taken by a government or public authority, including imposing an export or import restriction, quota or prohibition, or acts of terrorism (collectively, a "**Force Majeure Event**"), the Party so affected shall be excused from such performance and liability to the extent of such prevention or restriction. In the event that a third-party vendor of Ping Identity, such as a hosting provider, terminates or suspends its services to Ping Identity, or such services are otherwise materially impacted outside of Ping Identity's reasonable control, Ping Identity may suspend its provision of the Services to Customer for the duration of such occurrence. In such event, Ping Identity will promptly use commercially reasonable efforts to establish alternate facilities and/or services, as a replacement. **Anti-Bribery.** Ping Identity agrees not to provide, and Customer agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any Ping Identity employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If either Party learns of any violation of the above restriction, such Party will use reasonable efforts to promptly notify the other Party. Customer agrees to comply with all relevant anti-bribery and anti-corruption laws in effect in the UK and U.S. and its local regulations, if any.

12.13 Insurance. Throughout the term of this Agreement, Ping Identity shall, at its own cost, maintain reasonable insurance coverage. Ping Identity shall provide evidence of such insurance to Customer upon written request.

12.14 Headings, Advice of Counsel, and Drafting. Headings used in this Agreement are provided for convenience only and will not in any way affect the meaning or interpretation of each section. The Parties acknowledge that they have been advised by counsel of their own choosing, or had the opportunity to seek such counsel, and that its terms will be interpreted without any bias against one Party as drafter.

12.15 Ping Master Service Agreement. The Ping Master Service Agreement, including all of its exhibits governs Customer's usage of Ping Identity's Products under this Contract. All prior agreements between the Parties (including any click-through agreement associated with the Products), promises, assurances, understandings, proposals or representations, written or oral, concerning the subject matter contained in this Agreement, are expressly superseded by this Agreement. In entering this Agreement, neither Party has relied upon any statement, promise, assurance, understanding, representation, warranty, or agreement of the other Party except for those expressly contained in this Agreement. The U.N. Convention on the International Sale of Goods shall not apply to this Agreement.

12.16 Modifications, Amendments and Waivers. This Agreement may not be modified except by written instrument signed by both Parties.

12.17 Counterparts. This Agreement and any Order Forms may be executed by PDF or other electronic means, and in one or more counterparts, which taken together shall form one legal instrument.

12.18 Definitions.

(a) "**Affiliate**" means, with respect to any person, any other person directly or indirectly controlling, controlled by, or under direct or indirect common control with such person. Notwithstanding the foregoing, with respect to Ping Identity, the term "Affiliate" shall not include any commingled funds or investment vehicles managed by a registered investment advisor (or any portfolio company thereof) or any other person principally in the business of making or managing investments.

(b) **“Confidential Information”** means all confidential and proprietary information of a Party (the **“Disclosing Party”**) disclosed or made available to the other Party (the **“Receiving Party”**), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information or the circumstances of disclosure, the Products, the Customer Data, business and marketing plans, technology and technical information, pricing information, financial results and information, product designs, product roadmaps, results of penetration testing, security reports or audits and business processes.

(c) **“Customer Data”** means all electronic data or information provided to the Service in connection with Customer’s and its Users’ use of the Service. Customer Data may include Personal Information.

(d) **“Deliverables”** means, as applicable, those materials and/or solutions that Ping Identity provide to Customer pursuant to a SOW, expressly excluding Products.

(e) **“Documentation”** means Ping Identity’s then current on-line administrator user’s manuals for the Products made generally available by Ping Identity on its website.

(f) **“Intellectual Property Rights”** shall mean all existing and future worldwide copyrights (including, without limitation, rights in audiovisual works and moral rights), trademarks, service marks, trade names, patents, patent applications (including, without limitation, all reissues, divisions, renewals, extensions, continuations and continuations-in-part), inventions (whether patentable or not), trade secrets, know-how and any other proprietary rights whether arising under the laws of the United States, or any other country, state or jurisdiction.

(g) **“Malicious Code”** means viruses, worms, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

(h) **“Marketplace”** means the marketplace offered by Amazon Web Services, Inc. or its affiliates, or any similarly structured marketplace that Ping Identity may participate in from time to time.

(i) **“Order Form”** means any ordering document, including any product specific terms, supplements, or addenda thereto, for Customer’s purchases from Ping Identity that is executed by both Parties. Each Order Form is incorporated into the terms of this Agreement.

(j) **“Personal Information”** has the meaning assigned to it in the DPA.

(k) **“Products”** means the Software and Service.

(l) **“Professional Services”** means any administration, training, installation, health check, or similar professional services purchased by Customer as set forth in an Order Form and/or SOW.

(m) **“Reseller”** means a third party that has an agreement with Ping Identity that authorizes such third party to resell Products, Professional Services, or Support Services to Customer.

(n) **“Service”** means hosted, software-as-a-service offerings provided by Ping Identity that are identified on an Order Form or otherwise made available to Customer.

(o) **“Software”** means the downloadable software programs offered by Ping Identity that are identified on an Order Form or otherwise downloaded or installed by Customer, including in connection with its use of the Service.

(p) **“SOW”** shall mean a written document attached to an Order Form that describes the Professional Services to be performed to be completed.

(q) **“Subscription Term”** means the duration set forth for which Customer is permitted to use the Products, as set forth on an Order Form.

(r) **“Users”** means any administrator of Customer and individuals (including non-human devices) who are provisioned by Customer (or Customer’s authorized third parties accessing Customer’s services) to utilize the Products, or with whom Customer utilizes the Products, in connection with Customer’s use of the Products. Order Forms define the specific number and type of Users that Customer is authorized to permit to utilize the Products.

Exhibit A
Ping Identity Support Policy

This Ping Identity Support Policy (this "**Policy**") describes Ping Identity's Support Services, as referenced in the agreement to which this exhibit is attached (the "**Agreement**").

1. Responsibilities.

1.1. During the Subscription Term, Ping Identity shall, in accordance with Section 2 of this Policy:

- (a) provide Customer access to all generally available updates, upgrades, enhancements, fixes, and new versions of the Software;
- (b) respond to and Resolve all Errors;
- (c) maintain Uptime Availability for the Service of 99.99%;
- (d) provide unlimited telephone support to Customer during all Support Hours; and
- (e) provide Customer with online access to a support portal ("**Support Portal**"). The Support Portal may include a case submission form, case status and history, security advisory history, license history, access to download licensed Products, knowledge base articles, and Documentation.

1.2. During the Subscription Term, Customer shall:

- (a) provide prompt notice of any Errors via the Support Portal (each, a "**Support Request**"). Customer shall include in each Support Request a description of the reported Error and the time Customer first observed the Error;
- (b) cooperate and assist Ping Identity in Resolving the Support Request by taking any reasonably necessary actions that Ping Identity may request, including but not limited to, reproducing operating conditions similar to those present when Customer detected the Error and providing relevant data, documents, and information;
- (c) designate in writing to Ping Identity certain individual(s) at Customer who will provide timely and accurate information to Ping Identity in connection with a Support Request or Support Services;
- (d) notify Ping Identity reasonably in advance of any material modifications or adaptations to the configuration or implementation of the Ping Identity Products. This includes, without limitation, integration of third-party resources or changes that could affect volume or throughput, such as adding a significant number of applications or a significant enrollment event; and
- (e) test any planned upgrades in lower environments prior to a production upgrade.

2. Customer Support and Severity Levels. The Support Services details and levels are set forth below. Ping Identity shall respond to Support Requests in accordance with the applicable Severity Level and Response Time. The Response Times are measured only during Support Hours. Ping Identity will use commercially reasonable efforts to Resolve the Support Request in a prompt manner following its receipt of the Support Request, taking into account the Severity Level of the Error. Unless Customer has purchased an active subscription for Select, Premium or Elite, Customer will be entitled to Base Support.

Support Offerings		Base	Select	Premium	Elite
Multi-channel Technical Support <i>Access to technical support via phone and support portal</i>		✓	✓	✓	✓
Software downloads, Updates, and Maintenance <i>Access to the latest releases to take advantage of the newest features</i>		✓	✓	✓	✓
Access to Support Portal Knowledgebase and Community <i>Access to the support knowledgebase and community portal for on-demand information and assistance at any time</i>		✓	✓	✓	✓
Response Times	Severity 1	2 Hours	1 Hour	30 Minutes	15 Minutes

Support Offerings	Base	Select	Premium	Elite
Severity 2	4 Hours	3 Hours	2 Hours	1 Hour
Severity 3	24 Hours	12 Hours	8 Hours	4 Hours
Severity 4	48 Hours	36 Hours	24 Hours	12 Hours
Support Account Management <i>A team of advocates to monitor cases and assist with escalations</i>			✓	✓
Technical Account Manager <i>Up to 20hrs per month with a cross-functional advisor to aid in long-term strategy and ROI</i>				✓
Dedicated Support Team <i>Dedicated support staff to manage cases and engage engineering when needed</i>				✓
VIP Phone Number <i>Dedicated number to access senior technical resources</i>				✓
Expedited Support Experience <i>Jump queue to accelerate case resolution</i>				✓

Customer Success				
Named Customer Success Resource <i>Works with the Customer to ensure that the Customer is receiving the tools and support needed to achieve its goals</i>		✓	✓	✓
Pulse Cadence <i>Regularly scheduled meetings for collaboration to achieve success</i>		Quarterly	Monthly	Twice Monthly
Success/Milestone Alignment <i>Manage short- or long-term objectives and measure success against the Customer goals</i>		Twice Yearly	Quarterly	Quarterly
Executive Business Review <i>Strategic meeting with stakeholders and decision makers from both Ping Identity and the Customer</i>		Yearly	Twice Yearly	Twice Yearly
Innovation & Roadmap Sessions <i>Discussion of the Customer vision and how to align with the future roadmap for success</i>		Yearly	Twice Yearly	Twice Yearly
Value Unlock Forum <i>Identifying the white space between what the Customer is doing and what the Customer could do with current license(s)</i>			Yearly	Yearly

Professional Services				
Prepaid Service Advisory Hours <i>Includes all Professional Services packages except Partner Expert Services Packages and any bespoke SOW engagement</i>			10% Discount	10% Discount

Training				
Training All Access Subscription (Individual) <i>Two (2) individual passes for full access to the Ping Identity combined training offerings</i>		10% Discount	20% Discount	30% Discount

On-Demand Product Training <i>Access to online learning resources & library</i>	✓	✓	✓	✓
Automated Skills Assessment <i>Analyzes the skill level of the Customer delegates and suggests appropriate product training</i>			✓	✓

3. **Supported Releases for Products.** Ping Identity provides Support Services for the versions of the Products as set forth in its End of Life Policy as Addendum 2 below (the “**End of Life Policy**”).

4. **Exclusions.** Custom Developments and Out-of-Scope Services are not subject to this Policy. Ping Identity shall provide Support Services for Custom Developments and Out-of-Scope Services only upon the mutual written agreement between Ping Identity and Customer, including any fees related thereto. In addition, Ping Identity may offer optional value-added functions, features, or other capabilities related to the Products for a separate fee, and any such items are not automatically provided with the base Product under Section 1.1(a) of this Policy.

5. **Reserved.**

6. **Customer Success.** Customers in the Select, Premium and Elite support tiers will be assigned a Customer Success resource (“CSx”). The CSx shall function as a management-level liaison and point of contact between Customer’s organization and the different teams within Ping Identity.

6.1. The CSx will provide the services set forth in the table under Section 2 above. Specific details, including but not limited to timing, scheduling, and determining the number of specific meetings or sessions, are subject to Customer support level as well as the CSx’s reasonable discretion taking into account Customer’s particular circumstances, Customer’s reasonable requests, and any other relevant factors.

6.2. The CSx will be available Monday through Friday during regular business hours (or after hours if coordinated accordingly) as reasonable taking into account location and availability.

6.3. The following services are expressly excluded from the CSx services hereunder:

- (a) A CSx is not a technical resource and will not work on Customer’s technical issues, but they can interface with the support team to convey prioritization of Customer issues and/or escalation of open tickets;
- (b) A CSx will not manage projects for Customer but can assist in providing recommendations to Customer as well as inform internal Ping Identity teams on Customer’s project timelines; and
- (c) A CSx is not a support contact. Customer’s first point of escalation for Errors is the Support Portal.

7. **Reserved.**

8. **Definitions.** Capitalized terms used in this Policy shall have the meaning ascribed to such terms as set forth below or as otherwise defined in this Policy. Any capitalized terms not otherwise defined in this Policy shall have the meanings given to such terms in the main license or subscription agreement between Ping Identity and Customer (a “**Main Agreement**”).

8.1. **“Business Day”** means Monday through Friday, excluding weekends.

8.2. **“Core Components”** means those aspects of the Service that if unavailable would result in the complete interruption of a production system that impacts all users where no viable workaround exists.

8.3. **“Custom Developments”** mean custom software, materials, or solutions designed to interact with the Products developed by (a) Customer, with or without Ping Identity’s assistance, including the use of application programming interfaces (APIs) or other development tools related to the Products; or (b) Ping Identity for the benefit of Customer.

8.4. **“Customer Cause”** means: (a) any negligent or improper use (including improper installation or implementation), misapplication, misuse or abuse of, or damage to, the Products by Customer or any of its Representatives; (b) any maintenance, update, improvement or other modification to or a iteration of Products by Customer or its Representatives that was not specifically authorized in writing by Ping Identity; (c) any use of the Products by Customer or its Representatives in a manner inconsistent with the then-current Documentation; (d) any use by Customer or its Representatives of any third-party software, computer hardware, network hardware, electrical, telephone, wiring and all related accessories, components, parts and devices that Ping Identity has not provided to Customer; (e) any use by Customer or its Representatives of a version of the Products that is not supported under the End of Life Policy; or (f) any issue caused by Customer’s information technology infrastructure, including computers, software, databases, electronic systems (e.g., database management systems) and networks.

- 8.5. **"Error"** means any reproducible failure of the Products to operate in all material respects in accordance with the then-current Documentation, provided that the issue is not due to a Customer Cause.
- 8.6. **"Out-of-Scope Services"** means any of the following: (a) any services requested by Customer for Products for which Customer has not purchased or paid for Support Services; (b) any services requested by Customer in connection with any apparent Error that Ping Identity determines in its reasonable discretion to have been caused by a Customer Cause; or (c) any other services that Customer and Ping Identity may from time to time agree in writing are not included in the Support Services.
- 8.7. **"Representative"** means any employee, contractor, or agent of Customer or an Affiliate of Customer.
- 8.8. **"Resolve", "Resolved", "Resolution"** and correlative capitalized terms mean that Ping Identity has corrected the Error, whether by a work-around or any other reasonable means, that prompted that Support Request.
- 8.9. **"Response Time"** means the time from when Ping Identity receives a Support Request until Ping Identity has acknowledged receipt of that Support Request.
- 8.10. **"Severity Level"** means the level of severity assigned to an Error. Ping Identity shall assign the respective Severity Level to an Error, subject to the parties' written agreement to revise such designation after Ping Identity's investigation of the reported Error and consultation with Customer.
- 8.11. **"Severity Level 1"** means the Error results in complete interruption of a production system that impacts all or a majority of users and no viable workaround exists, or an event that impacts Uptime Availability. Customer may call Ping Identity to report a Severity Level 1 Error.
- 8.12. **"Severity Level 2"** means the Error does not impact Uptime Availability, but has a severe impact on performance, important services/components are not functioning, or a subset of users cannot access necessary functionality in a production system.
- 8.13. **"Severity Level 3"** means the Error (i) has a low impact on a small number of users in a production environment; or (ii) impacts a non-production environment; or (iii) general how-to questions for when a minor issue is impacting usability or administration of an environment.
- 8.14. **"Severity Level 4"** means Customer is informing Ping Identity about a minor problem or enhancement request for which feedback is not required.
- 8.15. **"Support Hours"** means (a) for Base level support: 24x7 for Support Requests related to Severity 1 Errors, and normal business hours on Business Days for Support Requests related to Severity 2, Severity 3 and Severity 4 Errors; (b) for all other support levels: 24x7 for Support Requests related to Severity Level 1 and Severity Level 2 Errors, and normal business hours on Business Days for Support Requests related to Severity 3 and Severity 4 Errors.
- 8.16. **"Uptime Availability"** means the uptime of the Core Components of the Service, measured per calendar year. Uptime Availability does not include downtime that results from a Customer Cause or a Force Majeure Event.

Addendum 1

Ping Identity Support Policy Addendum for Single-Tenant Services

1. **Scope.** This Addendum applies solely to Customer's use of any Services that are provided by Ping Identity as a dedicated single-tenant solution (as opposed to multi-tenant SaaS) ("**Single-Tenant Services**"), and in the event of a conflict between this Addendum and the Support Policy, this Addendum controls. This Addendum does not apply to Customer's use of any Products other than Single-Tenant Services.

2. **Customer Responsibilities.** In addition to the obligations in the Support Policy, Customer is required to notify Ping Identity reasonably in advance, through the Service Request process, of any material modifications or adaptations to the configuration or implementation of the Single-Tenant Services. This includes, without limitation, integration of third-party resources or changes that could affect volume or throughput of Single-Tenant Services, such as adding a significant number of applications or a significant enrollment event. Additionally, Customer is responsible for testing any planned upgrades in lower environments prior to a production upgrade. Customer must provide Ping Identity with written notice of any potentially production-impacting issues found in lower environments at least three business days prior to a scheduled production upgrade. If no notice is provided, Ping Identity will proceed with the scheduled upgrade with the assumption that Customer has performed reasonable testing of the release.

3. **Service Updates.** From time to time, Ping Identity may apply (a) patches, fixes or other updates that are designed to remediate potential security vulnerabilities, performance issues, or other issues, and (b) platform upgrades (including infrastructure updates and version upgrades of each of the Software programs underlying Single-Tenant Services). Where Ping Identity believes such changes are likely to have a material detrimental effect on an environment:

(a) Ping Identity will provide reasonable advance notice to Customer for development, test and staging environments;

(b) for production environments, Ping Identity will work with Customer to schedule the updates or upgrades at an agreed time as soon as is reasonably possible. If Customer (i) does not schedule the updates or upgrades within ten (10) days from notice or (ii) does not provide notice of issues in the lower environments (per Section 2 above) at least three business days before the scheduled production upgrade, then Ping Identity will not be responsible for any related damages or liabilities under the Agreement or otherwise, and Ping Identity is permitted to perform the updates or upgrades at any time without responsibility for any resulting impact on Uptime Availability; and

(c) for material security or performance risks, Ping Identity may apply an update or upgrade without advance notice.

4. **Miscellaneous.**

(a) A "**Service Request**" means an administrative task related to the set-up or configuration of Single-Tenant Services. Service Requests do not constitute Errors under the Support Policy. Ping Identity will acknowledge receipt within one (1) Business Day of Customer's submission of a Service Request and use good faith efforts to address the Service Request within a reasonable time frame after Ping Identity's receipt of the Service Request, based on the nature and magnitude of the request.

(b) Customer is not entitled to separately download Software programs underlying Single-Tenant Services unless separately licensed for those Software programs on an individual basis.

(c) Customer must always run Supported Releases of the Software programs underlying Single-Tenant Services.

(d) The Uptime Availability requirement under the Support Policy only applies to production environments, and does not include windows for planned maintenance, upgrades and updates that are scheduled in advance between Ping Identity and Customer.

(e) The following additional provisions will be added to the definition of "Customer Cause" under the Support Policy: (i) failure by Customer to notify Ping Identity of material changes to Single-Tenant Services as required under Section 2 of this Addendum or to accept updates, patches or fixes as required under Section 3 above; (ii) changes by Customer to the configuration of Single-Tenant Services that impact its ability to communicate with other components, impacts performance and/or limits or eliminates service function; (iii) additions or modifications to configuration in Single-Tenant Services that require new or changed monitoring configuration, if such changes are implemented in a production environment before monitoring configuration is completed; and (iv) failure of services or applications not deployed on Single-Tenant Services, including without limitation Products hosted on Customer or third party systems.

Addendum 2: End of Life Policy

This End of Life Policy (the “**Policy**”) describes the intended communication and transition plans for discontinued Software, versions, features and 3rd party support, and provides information required to plan for migration to replacement technologies. For purposes of clarity, this Policy does not apply to Hosted Services. Any questions arising as to the interpretation of this Policy or the application of this Policy shall be as determined by Ping Identity in its reasonable discretion. Any conflict between this Policy and the terms of the Ping Identity Support Policy (the “**Support Policy**”) that incorporates this Policy shall be controlled by the provisions of this Policy. This Policy is effective for all new Software or releases of existing Software, regardless of release date or Support Services purchase date. All capitalized terms used but not otherwise defined herein shall have the meanings assigned to them in the Support Policy.

1. *Software Releases*

- Release Definitions:
 - “**Major Release**” means a new release of the Software that may introduce major new functionality, remove redundant or previously deprecated functionality, deprecate additional functionality that will be removed in the future, consolidate bug fixes from previous releases and/or contain architectural changes that require a review of deployment topology.
 - “**Minor Release**” means a new release of the Software that may introduce new features, enhance existing features, deprecate functionality that will be removed in the next Major Release and bug fixes.
 - “**Maintenance Release**” means bug fixes and security fixes. A Maintenance Release that includes only bug fixes requires no configuration changes; it is designed as a drop-in cumulative release on top of Software versions in Active Maintenance. A Maintenance Release that includes security fixes may introduce breaking changes; this will be clearly noted in the accompanying security advisory and release notes. The contents of Maintenance Releases are determined in Ping Identity’s sole discretion but typically include: (i) Fixes for Errors and Security Issues and (ii) Fixes for customer reported issues.
- The Software product version numbering scheme is defined as follows.
 - [Major].[Minor].[Maintenance]. Example: 7.1.2, where Major Release is 7, Minor Release is .1, and Maintenance Release is .2.

2. *Software Support Lifecycle*

The Software Support Lifecycle is based on an industry standard Short-Term Support and Long-Term Support model where a particular release version will be designated as either Short-Term Support or Long-Term Support. Each version of Software covered by the Software Support Lifecycle can be aligned to a clear stage in its lifecycle. These stages are: (1) Active Maintenance, (2) End of Maintenance, (3) End of Support, (4) End of Life.

- Short-Term Support Version:
 - Short-Term Support versions are particularly suited for environments where early access to new functionality is critical.
 - Short-Term Support versions remain in Active Maintenance for one (1) year following the release of the next version, regardless of whether the next version is another Short-Term Support release or a Long-Term Support release. During this period, the Short-Term Support version continues to receive Maintenance Releases.
 - At expiration of the Active Maintenance period, the Short-Term Support version transitions to End of Maintenance for a period of one (1) year. During this period, the Short-Term Support version is supported but no further Maintenance Releases will be provided.
 - At expiration of the End of Maintenance period, the Short-Term Support version reaches End of Life. At this point, the Short-Term Support version is no longer supported and no support, fixes or updates will be provided. Effectively, Short-Term Support versions reach End of Life two (2) years after the release date of the next version.
 - Extended Limited Support is not available for Short-Term Support versions.
- Long-Term Support Version:
 - Long-Term Support versions are particularly suited for critical environments where consistent performance and extended security are paramount.

- Long-Term Support versions remain in Active Maintenance for one (1) year following the release of the next Long-Term Support version; with a guaranteed minimum Active Maintenance period of three (3) years for each Long-Term Support version. During this period, the Long-Term Support version continues to receive Maintenance Releases.
 - At expiration of the Active Maintenance period, the Long-Term Support version is categorized as End of Support unless Customer purchases Extended Limited Support for an additional one (1) year of support.
 - At expiration of the Extended Limited Support period, the Long-Term Support version will be categorized as End of Life.
- Embedded Components: Ping Identity Software may contain embedded versions of other Ping Identity products. When a product has been embedded and distributed as a part of another Ping Identity Software release, the Software Support Lifecycle that applies to the top-level Software release will apply to all embedded versions as well.
 - Integration Kits: Upon release of a new version of an Integration Kit, the previous version of the same Integration Kit automatically enters an End of Support period for one (1) year. At the end of the one (1) year period, the Integration Kit will no longer be eligible for Support Services. Defect fixes are applied only to the current version of an Integration Kit.
3. **Security Note:** Maintenance of Customer's Ping Identity Software deployment is vital to its on-going security. In order to keep a deployment secure, Customer should: (1) respond to security advisories, (2) take immediate action where necessary, (3) upgrade to a supported version of the Software and (4) stay up to date with Maintenance Releases.

4. **Software Notices**

Ping Identity will use commercially reasonable efforts to provide:

- At least six (6) months' notice of an affected Software's End of Sale Date. End of Sale Date notification is limited to situations in which Ping Identity is retiring an entire Software product.
- At least eighteen (18) months' notice of an affected Software's End of Life Date. This notice only applies to full Software products being deprecated. End of Life Dates for versions of Software occurs automatically and is as set forth above in the section titled "Software Releases."
- At least twelve (12) months' notice prior to the End of Life Date for third-party capabilities or Software features that cease to be supported by the Software.
- At least six (6) months' notice prior to the End of Life Date for mobile devices, ecosystem related third party capabilities or features.

5. **Extension of Support Terms – Extended Limited Support**

5.1 Ping Identity offers the option to purchase a reduced support offering for Long-Term Support versions that are categorized as End of Support but have yet to reach End of Life. Extended Limited Support will be made available at an additional cost to Customer but only if Customer has a current Support Service subscription in effect. Extended Limited Support contracts are limited to a one (1) year term.

5.2 Extended Limited Support includes:

- Ability to raise Support Requests, subject to Customer's standard Response Time;
- Fixes for Errors designated as Severity Level 1 as defined in the Support Policy, where commercially reasonable;
- Fixes for Security Issues reported as Critical or High, where commercially reasonable;
- Access to Knowledge Base articles; and
- Access to the latest Software releases.

5.3 Extended Limited Support does not include:

- Product/feature enhancement requests;
- Functionality or design changes;
- Additional Maintenance Releases;
- Fixes for Errors designated as Severity Level 2 and below as defined in the Support Policy;
- Fixes for Security Issues reported as Medium or Low;
- New operating system support; or
- Service level commitments tied to Resolution Times related to Errors in the applicable Software.

6. *Documentation*

Ping Identity, to the best of its ability, provides up-to-date Documentation for all Software versions in Active Maintenance. Once a Software version transitions to End of Maintenance, or any subsequent lifecycle stage, the associated Documentation will remain accessible but will no longer receive updates for general enhancements or bug fixes.

7. *Definitions*

“**Active Maintenance**” means that the applicable Software/Software version is under active development by Ping Identity and is maintained and supported; during the Active Maintenance phase, Ping Identity offers Maintenance Releases and Support Services under the Support Policy.

“**End of Life**” or “**EOL**” means that the applicable Software/Software version is no longer maintained or supported; following an EOL designation, the Software/Software version, will no longer be improved, enhanced or supported, or otherwise eligible for Support Services under the Support Policy or Extended Limited Support.

“**End of Life Date**” means the date that the applicable Software/Software version is designated as End of Life.

“**End of Maintenance**” or “**EOM**” means that the applicable Software/Software version, is no longer maintained; following the EOM designation the Software/Software version will no longer be maintained but will still be eligible for Support Services under the Support Policy; Ping Identity may, in its sole discretion, provide patches or workarounds to address Critical Issues.

“**End of Sale Date**” means the date the applicable Software/Software version is no longer Generally Available.

“**End of Support**” or “**EOS**” means that the applicable Software/Software version is no longer maintained or eligible for Support Services under the Support Policy; Customer may elect to purchase Extended Limited Support on Long-Term Support versions, unless the Software has an EOL designation.

“**End of Support Date**” means the date the Software is no longer eligible for Support Services under the Support Policy.

“**Extended Limited Support**” means an individually negotiated Software support contract requiring a Ping Identity approved Order Form for a Software/Software version where Customer requests and purchases support beyond the applicable End of Support Date.

“**Fixes**” means an update designed to address specific issues within a Software/Software version; the delivery mechanism is determined at Ping Identity’s sole discretion and will vary based on product architecture, nature of the issue, release practices and other technical considerations.

“**Generally Available**” means a Software is generally available for sale and to receive Support Services on Ping Identity’s current price books.

“**Hosted Services**” or “**Services**” means hosted, software-as-a-service offering provided by Ping Identity.

“**Patch**” means a temporary fix provided to an individual customer to address a specific set of Errors until a permanent fix is made available in a Major, Minor or Maintenance Release; patches cannot be shared with other customers and are provided at Ping Identity’s sole discretion.

“**Security Issues**” means a technical vulnerability in the Software; Ping Identity applies criticality in accordance with NIST guidelines for CVSS v3 (i.e., Critical, High, Medium & Low).

“**Software**” means any of the downloadable software programs offered by Ping Identity that are identified on an order form or otherwise downloaded or installed by Customer.

“**Support Services**” means the Ping Identity support services for the Software as set forth on the applicable order form and governed by the Support Policy.

Exhibit B
Ping Identity Software Information Security Exhibit

This Ping Identity Software Information Security Exhibit (“**Exhibit**”) is incorporated into the agreement to which this Exhibit is attached (the “**Agreement**”). Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Agreement.

1 Defined Terms

1.1 Definitions

- 1.1.1 As used in this Exhibit, “Applicable Law” means all legal, regulatory or industry requirements applicable to performance under the Agreement or Order Form including the data protection or privacy laws of any applicable jurisdiction.
- 1.1.2 “Commercially Reasonable Efforts” means, in addition to the implied duty of good faith and fair dealing, at least those diligent measures that people experienced in the relevant subject area would generally regard as sufficient to constitute reasonable diligence for regulated financial institutions in relevant circumstances. In no circumstance shall techniques, tools or protocols publicly known to be deprecated or otherwise compromised be considered reasonable or secure under this definition.
- 1.1.3 “Disaster” means any sudden, unplanned catastrophic event that compromises Ping Identity’s ability to provide the Services including, without limitation, any other critical functions, processes, or services for some unacceptable period of time causing Ping Identity’s management to invoke their recovery plans.
- 1.1.4 “Disaster Recovery” means the collection of resources and activities to re-establish the delivery of the Services and the recovery and restoration of data lost by reason of the Disaster.
- 1.1.5 “Ping Identity System” means any physical or electronic system including, without limitation, applications, information stores, and infrastructure systems, used for storing, processing, or transmitting Customer Confidential Information.
- 1.1.6 “Intrusion Detection System” or “IDS” means any Ping Identity System that monitors a network or systems in real time for malicious activity or policy violations with such malicious activity or violations being reported either to an administrator or collected centrally using a security information and event management (SIEM) system that combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.
- 1.1.7 “Malware” means software programs designed to damage or perform other unwanted actions to or within any Ping Identity Systems. Such examples may include viruses, worms, Trojan horses, keystroke loggers and spyware.
- 1.1.8 “Multi-Factor Authentication” or “MFA” means authentication through verification of at least two of the following types of authentication factors: (i) knowledge factors, such as a username/password, or (ii) possession factors, such as token or text message on a mobile device, or (iii) inherence factors, such as a biometric characteristic.
- 1.1.9 “Recovery Point Objective” or “RPO”, also referred to as the “Maximum Data Loss”, means the targeted point in time from which it is necessary to recover Customer data in Ping Identity’s infrastructure and systems, and quantifies and the permissible amount of such data loss following an interruption caused by a Disaster, measured in hours.
- 1.1.10 “Recovery Time Objective” or “RTO” means the targeted elapsed time between the point of the interruption of the Services caused by a Disaster up to the point where the Services must be acceptably functional to Customer, measured in hours.
- 1.1.11 “Risk-Based Authentication” or “RBA” means any non-static authentication system which detects anomalies or changes in the normal use patterns of an individual and requires additional verification of the individual’s identity when such deviations are detected, such as using challenge questions.
- 1.1.12 “Security Incident” means any actual or reasonably suspected misuse, compromise, or unauthorized, accidental or unlawful acquisition, destruction, loss, alteration, disclosure, or access to Customer Confidential Information under the possession, custody, or control of Ping Identity Personnel including any circumstance pursuant to which Applicable Law requires either notification to be given to affected parties or other activity in response to such circumstance.
- 1.1.13 “Site” means any physical premise or Ping Identity Systems utilized by Ping Identity Personnel in performance of Services under the Agreement.
- 1.1.14 “Site Visit” means the physical or other access to Sites by Customer personnel, each a “Site Visitor”.
- 1.1.15 “Customer Confidential Information” means any data that is stored by Ping Identity on behalf of a customer within Ping Identity Systems during the fulfillment of a contract.

2 Information Management and Risk Management

2.1 Information Security Program

2.1.1 Ping Identity shall have and maintain a holistic information risk management program that complies with Applicable Law, incorporates reasonable and appropriate administrative, operational, technical, physical and organizational measures that are designed to preserve and protect the confidentiality, integrity and availability of Confidential Information. This program shall identify the organization's critical information, the threats associated with such information and maintain documented controls designed to mitigate anticipated risks for the same.

3 Access Control

3.1 Ping Identity Management of Access Control to Ping Identity Systems

3.1.1 For user accounts managed by Ping Identity that grant access to Ping Identity Systems that require material changes to such access, Ping Identity shall effect such changes in a timely manner.

3.1.2 For user accounts managed by Customer and utilized by Ping Identity Personnel that grant access to Customer Ping Identity Systems, Ping Identity shall notify the appropriate Customer security and access administration personnel of material changes to such access in a timely manner.

3.2 Encryption of Customer Confidential Information

3.2.1 Ping Identity shall use Commercially Reasonable Efforts to ensure that Customer Confidential Information is encrypted at rest and in transit.

3.3 Multi-Factor Authentication

3.3.1 For access to cloud-based or hosted Ping Identity Systems containing Customer Confidential Data, Ping Identity Systems shall, where possible, support Multi-Factor Authentication as a requirement for logon.

4 Incident Response Policy and Management

4.1 Response and Reporting

4.1.1 Ping Identity shall maintain an incident response plan and an incident response team with defined roles and responsibilities that are each periodically reviewed and authorized by appropriate management.

4.1.2 Ping Identity shall use Commercially Reasonable Efforts to anticipate, detect, evaluate, and respond to a Security Incident in a timely manner.

4.2 Incident Management and Forensics

4.2.1 Ping Identity shall use Commercially Reasonable Efforts to maintain relevant documentation related to Security Incidents including issues, outcomes, and remediation activities.

4.2.2 Ping Identity shall use Commercially Reasonable Efforts to maintain the integrity and chain of custody of relevant information related to Security Incidents and ensure that such information is preserved in a manner consistent with Applicable Law.

5 Secure Operations

5.1 Operational Management

5.1.1 Ping Identity shall use Commercially Reasonable Efforts to physically or logically segregate Customer Confidential Information from other non-Customer data within Ping Identity Systems.

5.1.2 Ping Identity shall use Commercially Reasonable Efforts to physically or logically segregate production, test and development Systems for which Ping Identity is responsible unless agreed to otherwise in writing by the parties prior to such use.

5.1.3 Ping Identity Systems used in the provision of Support Services shall be securely configured, maintained, and retired from use using Commercially Reasonable Efforts and incorporating, to the extent applicable, any legal, regulatory, and compliance requirements deemed necessary by Ping Identity in Ping Identity's reasonable judgment.

5.2 Anti-Malware

5.2.1 Ping Identity shall have an anti-Malware policy that requires Malware-detection software to be installed and enabled on Ping Identity Systems that interact with Customer Confidential Information and prohibits disabling such anti-Malware controls without appropriate authorization.

5.2.2 Ping Identity Systems shall be configured to automatically check for and automatically implement new anti-Malware signatures on a reasonable frequency.

5.3 Vulnerability and Patch Management

5.3.1 Ping Identity shall maintain effective vulnerability and patch management processes for Ping Identity Systems.

5.3.2 Ping Identity shall evaluate and effect appropriate remediation activities including the timely application of patches to impacted Ping Identity Systems in a risk-prioritized manner informed by such vulnerability detection processes.

5.4 Logging and Monitoring

5.4.1 Ping Identity shall log user actions related to Ping Identity Systems with the following requirements: (i) user and administrative actions, (ii) account privilege changes, (iii) all access attempts, (iv) configuration changes, (v) access to Customer Confidential Information, and (vi) changes to firewall and network access control systems.

5.4.2 Such logs shall be retained for an appropriate length of time and at least for the minimum retention period under Applicable Law and readily available for review by appropriate Ping Identity Personnel.

5.5 Intrusion Detection Systems (IDS)

5.5.1 Using Commercially Reasonable Efforts, for Ping Identity networks through which Customer Confidential Information traverses, Ping Identity shall utilize Intrusion Detection Systems and regularly update IDS signatures based on new threats which shall be applied in a timely risk-prioritized manner.

6 Remote Access to Internal Customer Ping Identity Systems

6.1 Administrative Requirements for Remote Access

6.1.1 Ping Identity shall require that remote users have valid non-disclosure obligations or other confidentiality agreements in force for such personnel prior to allowing such remote access.

6.1.2 Ping Identity shall maintain reasonable oversight of Ping Identity Personnel's use of such access.

6.1.3 Upon reasonable request, Ping Identity shall make available to Customer a complete list of Ping Identity Personnel accounts that have remote access privileges to Customer Systems.

6.1.4 Upon request by Customer, Ping Identity Personnel that have remote access to Customer Systems shall have confidentiality obligations which shall be acknowledged by signature.

6.1.5 Privacy training and information security training shall be completed by Ping Identity Staff prior to performance of Services and as required thereafter.

6.2 Technical Requirements for Remote Access

6.2.1 Ping Identity shall establish such connections through a mutually agreed facility between Parties and shall originate from Ping Identity's approved IP addresses and only through the use of Ping Identity's appropriately managed and approved devices.

6.2.2 Ping Identity shall utilize Commercially Reasonable Efforts to maintain the security of its Ping Identity Systems establishing such remote connections by appropriately applying the latest applicable security patches in a timely and risk-prioritized manner.

7 Disposal, Return and Retention of Customer Confidential Information

7.1 Disposal Requirements for Customer Confidential Information

7.1.1 Except as otherwise specifically required by Applicable Law or permitted by this Agreement, upon termination or expiration this Agreement and Customer's written request, or upon the reasonable written request of Customer, Ping Identity shall sanitize in a manner designed to make forensically unrecoverable by standard forensic technologies, using Commercially Reasonable Efforts, all Customer Confidential Information from all Ping Identity Systems, data retentive devices or any other media containing such Customer Confidential Information.

7.1.2 If Ping Identity discards or otherwise discontinues its use of media utilized at any time for the storage or processing of Customer Confidential Information, such media shall be made forensically unrecoverable in accordance with the relevant terms of such obligations as such obligations are set forth in the Agreement including this Exhibit.

7.1.3 Upon written request by Customer, Ping Identity shall represent its performance of applicable secure disposal obligations (e.g., NIST800-88 guidelines) by providing written attestation to appropriate Customer personnel in a timely manner. Notwithstanding any other provisions in the Agreement, Customer shall retain the right to assess, to its satisfaction, Ping Identity's performance of Ping Identity's secure data disposal obligations as such obligations are set forth in the Agreement and this Exhibit.

7.2 Return of Customer Confidential Information

7.2.1 Upon request by Customer, Ping Identity shall return copies of any Customer Confidential Information in its custody,

including in printed or physical form, to Customer in a format deemed usable by Customer.

7.3 Retention of Customer Confidential Information

7.3.1 Each Party shall be entitled to retain copies of the other Party's Confidential Information as may be required by the Party's record retention policy, audit requirements, or otherwise required to comply with Applicable Law, court order, warrant, subpoena, or other valid request carrying the force and effect of law, provided that (a) further processing, use or disclosure of such Confidential Information is limited to the purpose described in this Section and for no other purpose, (b) during such retention each Party agrees to treat such Confidential Information in accordance with the terms of the Agreement, and (c) such Confidential Information shall be retained only for such period as required by the purpose for which such Confidential Information was retained, as set forth in this Section and promptly returned, rendered permanently inaccessible, or destroyed in accordance with this provision upon the expiration of retention requirement. In no event shall Ping Identity withhold any Customer Confidential Information as a means of resolving any dispute between the Parties.

8. Information Contingency

8.1 Backup and Recovery

8.1.1 Ping Identity shall have policies and procedures for governing backup media that contain Customer Confidential Information which provide that:

8.1.2 Customer Confidential Information shall be retained for such period stipulated in the Agreement or other governing written agreement between Parties;

8.1.3 Such backups and replicas of data stores shall be treated with the same care and control as the stores in which such original information resides;

8.1.4 Access to such backup media shall be restricted to formally authorized Ping Identity Personnel and its access logged.

8.2 Business Continuity and Disaster Recovery Planning

8.2.1 Ping Identity's provision of Support Services shall be subject to an approved Business Continuity and Disaster Recovery (BC/DR) plan which is regularly reviewed by appropriate management.

8.2.2 To the extent applicable, such BC/DR plan(s) shall contain an appropriate strategy to meet the recovery objectives of Customer Confidential Information or the Services.

8.3 Business Continuity and Disaster Recovery Plan Requirements

8.3.1 The Business Continuity and Disaster Recovery (BC/DR) plan shall:

8.3.1.1 Include a mechanism designed to ensure the confidentiality, integrity, and availability of Customer Confidential Information during a Disaster;

8.3.1.2 For Support Services, meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) mutually agreed between Parties, but in no case longer than 48 hours for RTO and 12 hours for RPO unless otherwise specified in the Agreement or relevant Order Form;

8.3.1.3 Identify the technical and non-technical recovery actions and requirements that Ping Identity needs to perform when a Disaster is declared and when a recovery plan is executed; and

8.3.1.4 Identify the restoration procedure to switch production operations between primary and recovery sites and provide the corresponding validation process for such procedure.

8.3.2 Notwithstanding anything to the contrary in the Agreement, a *force majeure* event shall not excuse Ping Identity from its performance of its Disaster recovery obligations under Ping Identity's BC/DR plan or as such obligations are set forth herein.

8.4 Testing Requirements

8.4.1 Ping Identity shall conduct appropriately scoped BC/DR tests at least annually and address findings related to its performance of the BC/DR plan as they relate to the recoverability of Customer Confidential Information to meet the specified recovery objectives.

8.4.2 Upon request from Customer, Ping Identity shall provide to Customer a report, in a mutually agreeable format, after such relevant recovery exercises, that identifies the findings related to the recoverability of Customer Confidential Information and Ping Identity's actions, taken and planned, to address such findings.

8.4.3 Upon Customer's reasonable request, Ping Identity shall reasonably cooperate with any continuity risk or business impact analysis conducted by Customer to the extent applicable.

8.4.4 In lieu of the provisions contained hitherto in this Exhibit, upon Customer's reasonable request, Ping Identity shall furnish

to Customer such relevant third-party reports that sufficiently demonstrate assurance of the design and effectiveness of such testing and recoverability provisions to Customer's satisfaction.

9. Secure Development

9.1 Application Development Requirements

9.1.1 Ping Identity shall have and comply with a secure software development life cycle (SDLC) process that governs the development, testing, and maintenance of all applications used by Customer for storing, processing, or transmitting Customer Confidential Information or that comprise a component of the Service.

9.1.2 For such applications, threat modeling, including identification of threats during design, and application security testing including code scanning and manual penetration testing, shall be conducted for each major code release.

9.1.3 Ping Identity's application development and maintenance processes shall provide for continual testing of vulnerabilities within such applications with a commitment to provide patches on a schedule commensurate with the perceived risk associated with such corresponding vulnerabilities without adversely impacting the availability of related Ping Identity Systems.

9.1.4 To the extent Ping Identity utilizes open-source software on Ping Identity Systems or to deliver the Services, Ping Identity shall perform security due diligence activities using Commercially Reasonable Efforts with respect to the selection, acquisition, and maintenance of such open-source software to ensure appropriate risk mitigation practices including, without limitation, the application of timely security patching and vulnerability management oversight.

10. Human Resources Security

10.1 Employee Selection. To the extent reasonable, and permissible under Applicable Law, Ping Identity shall where appropriate, conduct, have conducted or otherwise require, background checks proportionate to the role for Ping Identity personnel performing Services under the Agreement including professional references and criminal background checks.

10.2 Ping Identity Personnel Security Management

10.2.1 Ping Identity shall maintain an acceptable use policy governing the use of computing resources including, without limitation, all Ping Identity Systems, that is communicated to appropriate Ping Identity Personnel.

10.2.2 Ping Identity shall require Ping Identity Personnel performing Services under the Agreement to maintain valid non-disclosure obligations or other confidentiality agreements as deemed reasonably necessary by Ping Identity.

10.3 Ping Identity Personnel Termination and Separation. Ping Identity shall have a process that governs the secure return of Ping Identity Systems and Customer Confidential Information for separated Ping Identity Personnel.

10.4 Training and Awareness. Ping Identity shall require that all Ping Identity Personnel complete upon hire and, at least annually thereafter, Ping Identity's security awareness training including a wareness of Ping Identity's related policies and maintain records of such training completion.

11. Compliance and Reporting

11.1 Regulatory Compliance. Ping Identity shall use Commercially Reasonable Efforts to comply with Applicable Law. Such compliance efforts shall be designed, managed, and regularly evaluated for effectiveness by qualified Ping Identity Personnel.

11.2 External Information Security Assessment and Certifications

11.2.1 Using Commercially Reasonable Efforts, Ping Identity shall have a reputable third party conduct an information security assessment upon the introduction of a new product or service, and for every major change to an existing product or service.

11.2.2 Up to once annually upon Customer's request, Ping Identity shall make available, and all information reasonably necessary to demonstrate compliance with its privacy, compliance, and information security obligations under the Agreement and this Exhibit. Such information may include Customer's information security questionnaire, SOC 2 Type II, ISO 27001 or other relevant compliance reports or certifications including high-level reports, in a mutually agreeable format, of external information security assessment findings to the extent such findings relate to Ping Identity Personnel's ability to safeguard Customer Confidential Information applicable to Ping Identity's performance of its obligations under the Agreement. Ping Identity shall use Commercially Reasonable Efforts to correct any material control deficiencies identified through such examinations, as described in this Exhibit, in a timely risk-prioritized manner.

Exhibit C
Ping Identity Service Information Security Exhibit

1. Security Policy Overview.

- 1.1. Ping Identity's Commitment to Security. Ping Identity is committed to achieving and preserving the trust of our Customers by providing a comprehensive security program that carefully considers data protection matters across our suite of products and services, including any Customer Data submitted by Customers to the Service.
- 1.2. Covered Services. This documentation describes the certifications held by Ping Identity, and the administrative, technical, and physical controls applicable to the Service. This exhibit does not apply to free trial services and beta versions made available by Ping Identity.
- 1.3. Ping Identity may update or modify these security practices from time to time provided such updates and modifications will not result in a material degradation of the overall security of the Service.

2. Default Security Controls and Information Security Management Program.

- 2.1. Default Security Controls. The Service includes a variety of configurable security controls that allow Ping Identity Customers to tailor the security of the Service for their own use. Ping Identity personnel will not set a defined password for a user. Each Customer's users are provided with a token that they can use to set their own password in accordance with the applicable Customer's password policy. Ping Identity strongly encourages all customers, where applicable in their configuration of the Service's security settings, to use the multi-factor authentication features made available by Ping Identity.
- 2.2. Information Security Management Program. Ping Identity maintains a comprehensive Information Security Management System ("ISMS") that contains administrative, technical, and physical safeguards that are appropriate to (i) the size, scope and type of Ping Identity's business; (ii) the amount of resources available to Ping Identity; (iii) the type of information that Ping Identity will store and process; and (iv) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMS is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service and reviewed at least annually. Ping Identity's ISMS is designed to:
 - (a) Protect the integrity, availability, and confidentiality, of Customer data in Ping Identity's possession or control;
 - (b) Protect against reasonably anticipated threats or hazards to the integrity, availability, and prevention of unauthorized disclosure of Customer Data by Ping Identity or its agents;
 - (c) Protect against unauthorized access, use, alteration, or destruction of Customer Data;
 - (d) Protect against accidental loss or destruction of, or damage to, Customer Data; and
 - (e) Safeguard information as set forth in any local, state or federal regulations by which Ping Identity may be regulated.
- 2.3. Security Standards. Ping Identity's ISMS includes adherence to and regular testing by internal and independent external audit of the key controls, systems and procedures of its ISMS to validate that they are properly implemented and effective in addressing the threats and risks identified. Ping Identity engages an independent third party to conduct an annual security testing of its controls. Ping Identity will maintain SOC 2 and ISO 27001 certifications or their equivalents during the term of the Agreement.
- 2.4. Policies and Standards. Ping Identity maintains policies or standards addressing the following areas which include but are not limited to: risk management, information security, acceptable use, access control, software development lifecycle, change control, vulnerability management, data classification, encryption, data retention, incident response, backup and recovery, and business continuity.
- 2.5. Risk Management. Ping Identity maintains a documented risk management program that includes a risk assessment at least annually approved by senior management.
- 2.6. Assigned Security Responsibility. Ping Identity assigns responsibility for the development, implementation, and maintenance of its ISMS, including:
 - (a) Designating a security executive with overall responsibility; and
 - (b) Defining security roles and responsibilities for individuals with security responsibilities within Ping Identity.

3. Relationship with Sub-processors. Ping Identity conducts reasonable due diligence and security assessments of sub-processors engaged by Ping Identity in the storing and/or processing of Customer Data ("**Sub-processors**") and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security documentation.

4. Disciplinary Policy and Process. Ping Identity maintains a disciplinary policy and process in the event Ping Identity personnel violate security policies.

5. Access Controls.

5.1 Access Control Policies and Procedures. Ping Identity has policies, procedures, and logical controls that are designed:

- (a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
- (b) To prevent personnel and others who should not have access from obtaining access; and
- (c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

Additionally, Ping Identity institutes:

- (d) Controls to ensure that only those Ping Identity personnel with an actual need-to-know will have access to any Customer Data;
- (e) Controls to ensure that all Ping Identity personnel who are granted access to any Customer Data are based on least-privilege principles;
- (f) Controls to require that user identifiers (User IDs) shall be unique and readily identify Ping Identity person to whom it is assigned, and no shared or group User IDs shall be used for Ping Identity personnel access to any Customer Data; and
- (g) Customer User Authentication. Password and other strong authentication controls are made available to Ping Identity customers, so that Customer can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user. Customers are responsible for the configuration and management of the authentication requirements for their end users.

5.2. Physical and Environmental Security. Data center physical and environmental security controls are managed by approved third parties who operate tier 4 and 5 data centers.

5.3. Privileged Access by Ping Identity. If Ping Identity determines, in its reasonable discretion, that there is a material and immediate risk to the availability, integrity, or security of Customer's data due to misconfiguration or a verified security incident, Ping Identity may use restricted privileged access accounts to access the data. In the event Ping Identity need to enter a Customer environment, Ping Identity shall use reasonable efforts to contact the Customer prior to any action being taken. Ping Identity reserves the right to effect access without Customer consent when contact attempts fail and/or immediate action is required to preserve service for one or more customers.. In the event of direct access to customer data, subsequently upon request the Customer will receive a report including: (i) when access took place; (ii) what actions were taken; and (iii) a post event review summarizing impact on the Customer and root cause analysis of the incident. Emergency access under this Section shall be limited to infrastructure-level operations and shall not include application-level access or intentional viewing of Customer content. Ping Identity shall not decrypt or access Customer content except to the extent strictly necessary to restore service or contain an incident, and only where technically unavoidable.

6. Data Encryption.

6.1. Encryption of Transmitted Data. Ping Identity uses industry-standard secure encryption methods designed to encrypt communications between the Service and its Users, Transmitted Customer data is encrypted using the latest supported industry standard cryptographic protocols such as Transport Layer Security ("TLS").

6.2. Encryption of At-Rest Data. Customer Data in the Service is encrypted at rest using industry standard encryption algorithms.

6.3. Encryption of Backups. All backups are encrypted. Ping Identity uses disk storage that is encrypted at rest.

6.4. Global Configuration Data: All configuration data is secured and encrypted.

6.5. Services Encryption: Where applicable, accounts are configured with their own unique key preventing assertions from other accounts from being processed. Audit logs track all Users who log in and which applications they access.

6.6. Ping Identity Personnel Equipment. Personnel endpoints provisioned by Ping Identity shall have the following:

- (a) Whole disk encryption
- (b) anti-malware and endpoint protection solutions
- (c) Strong password enforcement
- (d) Mobile device management

7. **Business Continuity and Disaster Recovery**. Ping Identity maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain such Customer Data. Such procedures include:

- (a) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;
- (b) Disaster Recovery: A disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, at least annually;
- (c) RPO / RTO applies as below:
 - i. For PingOne, PingOne for Enterprise/PingID and PingOne Advanced Services:

- Recovery Point Objective (“**RPO**”) is twenty-four (24) hours and Recovery Time Objective (“**RTO**”) is eight (8) hours;
- ii. For PingOne Advanced Identity Cloud only:
 - RPO/ RTO: Recovery Point Objective is no more than one (1) hour and Recovery Time Objective is no more than one (1) hour for production in-region recovery, and no more than four (4) hours for backup region disaster recovery;

(d) Business Continuity Plan: A process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

8. Secure Development Practices. Ping Identity adheres to the following development controls:

- (a) Development Policies: Ping Identity follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10, SANS Top 20 Critical Security Controls and applicable controls of the CIS Top 18;
- (b) Least Privilege: Only authorized Personnel with a specific business purpose shall be allowed access to production and development resources, and all access shall be appropriately approved;
- (c) Manual Code Review: Ping Identity requires a code review and peer review for all Services;
- (d) Automated testing: Ping Identity engineers are required to test each build prior to deployment to the production environment; and
- (e) Training: Ping Identity provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training regarding secure application development practices.

9. Data Integrity and Management. Ping Identity maintains policies that ensure the following:

- (a) Segregation of Data: The Service includes logical controls, including encryption, to segregate Customer Data from that of other customers; and
- (b) Back Up/Archival: Ping Identity performs regular backups of the database(s) containing Customer Data on a periodic basis, at least daily. Backups are stored in encrypted state.
- (c) Data Centers: The Service is provided through geographically distributed, redundant, and secure data centers (see clause 5.2 above) operated by third parties. Ping Identity relies on security controls of such parties and reviews their controls to confirm adequate controls are in place and designed to protect the confidentiality, integrity and availability of the Service.
- (d) All production servers are hardened, monitored, or have anti-malware protection software installed and updated periodically.
- (e) Customer Data Handling. Ping Identity maintains appropriate data security controls addressing the following areas which include but are not limited to:
 - Data classification;
 - Data leakage protection;
 - Technical controls to prevent the use of removable media;
 - Secure and integrity-checked data storage and transmission at rest and in-transit; and
 - Access, usage, and capacity monitoring and control.

10. Vulnerability Management. Ping Identity maintains security measures to monitor the network and production systems, error logs on servers. Such measures include:

- (a) Infrastructure Scans: Ping Identity performs regular vulnerability scans. Vulnerabilities are remediated on a risk basis. Ping Identity installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;
- (b) Application Scans: Ping Identity performs regular (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis;
- (c) Application Vulnerability Assessment: Ping Identity engages third parties to perform network and application vulnerability assessments, and penetration testing on at least an annual basis (“Vulnerability Assessment”). Executive reports from Ping Identity’s then-current external assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. Ping Identity installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

11. Penetration Testing.

11.1 **Third Party Penetration Test:** Ping Identity performs at least annual third-party penetration testing of the Services. An executive summary of the latest penetration test shall be made available upon Customer's written request.

11.2 **Customer Testing:** Customers are prohibited from performing penetration, load, or performance testing against the Services without Ping Identity's written approval. Customers may submit a written request for such testing and may be required to review applicable policy and provide written details, such as detailed test case, dates and times of testing, tester details, and other industry standard information.

11.3 **PingOne Advanced Identity Cloud:** Notwithstanding the above, penetration and load testing can only be performed on PingOne Advanced Identity Cloud. Customer may perform load testing that is representative of expected production volumes in the staging environment. Customer may perform penetration testing of their own environment in line with the requirements of the Ping Identity Cloud Penetration & Load Testing Policy located on the Ping Identity Customer Portal.

12. **Change and Configuration Management.** Ping Identity maintains policies and procedures for managing changes to production systems, applications, and databases for the Service. All changes must contain documentation and relevant rollback plans. Each change is reviewed, approved, and tested prior to Service deployment or software release.

13. **Secure Deletion.** Ping Identity maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted from data centers using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with NIST SP800-88 guidelines.

14. **Intrusion Detection.** Ping Identity monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. Ping Identity may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

15. **Incident Management.** Ping Identity has a security incident response plan that includes procedures to be followed in the event of unauthorized or unlawful access to or disclosure, loss, exposure or use of any Customer Data of which Ping Identity becomes aware (such unauthorized disclosure defined herein as a "**Security Breach**"). The procedures in Ping Identity's security incident response plan include:

- (a) Roles and responsibilities: formation of an internal incident response team with a response leader;
- (b) Triage: assessment of the risk and criticality of the incident to ensure correct prioritization and allocation of resources;
- (c) Analysis: analysis of each incident shall take place to determine the scope, spread, cause, mitigation and remediation of the incident;
- (d) Notification: internal and external stakeholders and customers who experience a Security Breach with material impact on their data or environment shall be notified without undue delay upon Ping Identity becoming aware of the Security Breach;
- (e) Containment: appropriate steps shall be taken to stop the incident and limit the damage or risk caused by the incident; and
- (f) Eradication: appropriate steps shall be taken to eliminate any remaining elements of the cause of the incident ;
- (g) Recovery: appropriate steps shall be taken to restore any and all affected systems to a functionally optimal state;
- (h) Documentation: all material actions taken during the incident response process shall be documented for internal analysis and communication to internal and external stakeholders and customers who experience a security breach with material impact on their data or environment;
- (i) Retrospective analysis: internal analysis of actions taken during the incident response process shall be reviewed by relevant stakeholders to determine the efficacy of the response process and document any further actions that may improve the operation of the incident response process if invoked in the future.

Ping Identity publishes system status information on the Ping Identity website. For PingOne Advanced Services and PingOne Advanced Identity Cloud only, Ping Identity typically notifies customers of significant system incidents by email to the listed admin contact, and for a availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Ping Identity's response.

16. Security Breach Management.

- (a) Notification. In the event of a Security Breach, Ping Identity notifies impacted customers of such Security Breach without undue delay, but no later than 72 hours and, where required, within time limits defined by law. Ping Identity shall cooperate with the Customer's reasonable request for information regarding such Security Breach, and Ping Identity provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.
- (b) No Acknowledgement of Fault by Ping Identity. Ping Identity's notification of or response to a Security Breach shall not be construed as an acknowledgement by Ping Identity of any fault or liability with respect to the Security Breach.
- (c) Remediation. In the event of a Security Breach, Ping Identity, at its own expense shall:
 - (i) investigate the actual or suspected Security Breach

(ii) where a breach impacts a Customer, provide affected Customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents,

(iii) remediate the effects of the Security Breach within Ping Identity's scope of control and

(iv) reasonably cooperate with Customer and law enforcement or regulatory official investigating such Security Breach.

17. Logs. Ping Identity provides procedural mechanisms that record and examine activity in the Service, including appropriate logs and reports. Ping Identity: (i) backs-up logs, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with Ping Identity's data retention policy.

18. Human Resources Security

18.1 Employee Selection. To the extent reasonable, and permissible under applicable law, Ping Identity shall where appropriate, conduct, have conducted or otherwise require, background checks proportionate to the role for Ping Identity personnel performing services under the Agreement including professional references and criminal background checks.

18.2 Ping Identity Personnel Security Management.

- (a) Ping Identity shall maintain an acceptable use policy governing the use of computing resources including, without limitation, all Ping Identity Systems, that is communicated to appropriate Ping Identity Personnel.
- (b) Ping Identity shall require Ping Identity personnel performing services under the Agreement to maintain valid non-disclosure obligations or other confidentiality agreements as deemed reasonably necessary by Ping Identity.

18.3 Ping Identity Personnel Termination and Separation. Ping Identity shall maintain personnel offboarding procedures that include revoking access promptly and a process that governs the secure return of Ping Identity assets and Customer Confidential Information for separated Ping Identity personnel.

18.4 Training and Awareness. Ping Identity shall require that all Ping Identity personnel complete upon hire and, at least annually thereafter, Ping Identity's security awareness training including a awareness of Ping Identity's related policies and maintain records of such training completion.

19. Security Audit Report and Assessment. This clause 19 is applicable during the Subscription Term and any information shared under this clause is Confidential Information subject to the confidentiality terms in the Agreement. This clause 19 is strictly limited to Customer's reasonable verification of Ping Identity's compliance with its obligations under this Service Security Exhibit.

19.1 Ping Identity provides its Customers, upon their request, with a summary of Ping Identity's then-current external audit report such as the ISO27001 Statement of Applicability, or, SOC 2 Report, including information as to whether the security audit revealed any material non-conformities in the Ping Identity Service. Ping Identity shall provide annually, or upon written request, evidence of third-party assessment and security reviews of its sub-contractors and sub-processors involved in providing the Service to Customer (collectively "**Third Party Audits**"). Ping Identity shall promptly inform Customer of any material issues identified as part of any Third-Party Audit which materially impact (or have the potential to materially impact) Customer. Ping Identity shall subsequently inform Customer of the actions it intends to take to remedy the relevant issues and the timeframe such remedial actions will be taken. Ping Identity shall consider any of Customer's reasonable observations in respect of the same and shall keep Customer regularly updated.

19.2 Ping Identity shall maintain records (as indicated in 19.1 above) relating to Ping Identity's obligations under this Service Security Exhibit as required under law which are applicable to Ping Identity's provision of the Service (including any electronic form) (the "Records"); and shall allow Customer to access and inspect Ping Identity's records as necessary to demonstrate Ping Identity's compliance with the obligations imposed under this Service Security Exhibit. This assessment may include one or more of the following as Customer may request: (i) responses to a reasonable information security-related questionnaire; (ii) the latest SOC 2 Type II audit report, (iii) the latest ISO 27001 certificate and ISO 27001 Statement of Applicability; (iv) an executive summary of the most recent penetration test of the Service and the status of findings not resolved during the test; (v) an executive summary of the most recent disaster recovery test of the Service; (vi) a summary of Ping Identity's operational practices related to data protection and security that Ping Identity normally shares with its other customers, which may include table of contents of key policies and procedures; and (vii) making Ping Identity's relevant personnel reasonably available for security-related discussions (subject to reasonable place, manner, scope, during normal business hours and not to exceed one (1) business day. The foregoing is strictly limited as follows: no more than once per year and contingent on an advanced written notice of twenty (20) business days of any such request.

19.3 Provided Customer has exhausted its rights above in sections 19.1 and 19.2, and upon reasonable cause and no more than once annually during the term of the Agreement, Customer may have access to Ping Identity's premises, information, data and relevant records, including any records it has retained in respect of this Service Security Exhibit to conduct a reasonable security assessment of whether the controls protecting Customer Data conform with Ping Identity's obligations under this Service Security Exhibit. Customer will work with Ping Identity to avoid impact on Ping Identity's systems or business processes and such audit shall be scheduled in advance subject to Ping Identity being provided at least sixty (60) business days advance written notice of the Customer's intention to audit, the audit being conducted during normal business hours, and in a timeframe mutually agreed in reasonable place, manner, and scope and not to exceed more than two (2) business days in order to enable Customer to:

(a) undertake verification that the Service is being provided in accordance with this Service Security Exhibit; and

(b) assess and verify Ping Identity's continued ability to comply with the obligations of this Service Security Exhibit (including, in respect of any operational resilience (except for penetration testing where relevant information shall be provided to the Customer in accordance with clause 10(c) above) and business continuity requirements in respect of the Service).

19.4 To the extent that Customer seeks an audit of Ping Identity's compliance with this Service Security Exhibit in addition to what is provided in 19.3 above, the parties agree to meet and confer in good faith on the understanding that the audit shall have the same scope as that provided in 19.3 above.

Exhibit D

Data Processing Addendum

Ping Identity Corporation agrees that it will comply with the following provisions with respect to all “Personal Information” collected, used, transmitted or maintained for Customer. This Data Processing Addendum (“DPA”) stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws.

This DPA is incorporated into and forms part of, and is subject to the terms and conditions of, the agreement to which this exhibit is attached (the “Agreement”). Any capitalized terms used in this DPA and not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1. Definitions.

- (a) “**AI Technology**” means any products, services or features that utilize machine learning software, algorithms, hardware or other artificial intelligence tools that generate content or make predictions, recommendations, or decisions.
- (b) “**CA Privacy Law**” means (collectively) the California Consumer Privacy Act, the California Privacy Rights Act, all implementing regulations, as and when effective, and any other applicable California state privacy laws.
- (c) “**Data Subject Request**” means any request by an individual (or by another person acting on behalf of an individual) to exercise a right under any Privacy Law or any complaint or inquiry about the Processing of the individual’s Personal Information.
- (d) “**Deidentified**” means a data set where (i) all Direct Identifiers have been removed, (ii) individuals cannot reasonably be identified using indirect identifiers in the dataset or using other information available to Ping Identity, and (iii) the data are protected by administrative and technical controls that are reasonably designed to ensure that the data are not re-identified or otherwise used in an identifiable manner. For purposes of this definition, a “Direct Identifier” is any single data element that could reveal a person’s identity, such as a person’s name, username or online identifier, email address, physical address or location, telephone number, device identifier, birthdate or transaction date, identification numbers (such as a government-issued ID number or account number) payment card number, IP address, biometric identifier, photograph or any other image that allows individual identification.
- (e) “**EEA Personal Data**” means that subset of Personal Information consisting of “personal data” (as defined in GDPR) pertaining to residents of the European Economic Area (EEA) and (for convenience) Switzerland and the United Kingdom.
- (f) “**GDPR**” means Regulation (EU) 2016/679 (the General Data Protection Regulation), including as it applies in UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018, and all applicable regulations, as and when effective.
- (g) “**Internal Business Purposes**” means processing of Personal Information by Ping Identity to (i) make back-ups as part of disaster recovery and business continuity programs; (ii) comply with its own legal or regulatory obligations; (iii) build and improve the quality of the Services, including debugging to identify and repair errors that impair intended functionality, provided that Ping Identity does not use Personal Information to provide services to other companies or to create profiles of individuals (other than for Customer or as needed to mitigate fraud and malicious activity); (iv) confirm usage quantities; and (v) prevent, detect or respond to security incidents or malicious, deceptive, fraudulent, or illegal activity.
- (h) “**Personal Information**” means all data (regardless of format) that (i) identifies or can be used to identify, contact, locate or target a natural person, (ii) pertains in any way to an identified natural person, or (iii) falls within any definition of “personal information” or “personal data” under any applicable Privacy Law, and that is processed by Ping Identity in connection with providing the Services to Customer.
- (i) “**Personal Information Breach**” means a “personal data breach” (as defined in the GDPR or other applicable Privacy Laws), any unauthorized use or disclosure of the Personal Information, or other event that compromises the security, confidentiality, or integrity of Personal Information.
- (j) “**Privacy Laws**” means all applicable laws that regulate the Processing of Personal Information. In particular, the Privacy Laws include (as applicable) the CA Privacy Laws, the GDPR, and other applicable U.S. Federal, state and international laws and regulations that specify privacy, data protection, security or security breach notification obligations or that otherwise regulate the Processing of the Personal Information or the provision of the services by Ping Identity.

- (k) **“Processing”** means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, deidentification, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.
- (l) **“Restricted Transfer”** means any Transfer where the applicable Privacy Law requires the parties to demonstrate adequate protection using a standard contractual instrument or other prescribed means. Restricted Transfers do not include Transfers to recipients in countries whose data protection regimes have been declared adequate by relevant data protection authorities or which are otherwise not restricted.
- (m) **“Services”** means all services Ping Identity provides to or performs for Customer that entail Processing of Personal Information. “Services” encompasses the processing services as well as any products, websites, applications, devices or technologies used in connection with the provision of the Services.
- (n) **“Standard Contractual Clauses”** means (as applicable) (i) the contract terms set forth in the Annex to the European Commission’s decision C(2021) 3972 of 4 June 2021 containing Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, or (ii) other contract terms published by relevant regulatory authorities to authorize data Transfers.
- (o) **“Subprocessor”** means any entity (including an Affiliate of Ping Identity) acting under the instructions of Ping Identity that processes unencrypted Personal Information on behalf of Ping Identity.
- (p) **“Transfer”** means to disclose or otherwise make the Personal Information available to another entity (including to any Ping Identity Affiliate or Subprocessor), either by physical movement of the Personal Information or by enabling remote access to the Personal Information.

2. General Obligations.

- (a) Each party must use reasonable efforts to stay informed of the legal and regulatory requirements for its applicable responsibilities under this DPA. Ping Identity will comply with those obligations applicable to it as a “data processor” or “service provider,” and Customer will comply with those obligations applicable to it as a “data controller” or “business” (each as defined in the applicable Privacy Laws). Customer shall be responsible for ensuring that it has, and will continue to have, the right to transfer, or provide access to, Personal Data to Ping Identity for Processing as set forth herein. If any authorizations or consents of data subjects are required for such Processing of Personal Data by Ping Identity, Customer shall obtain such consents directly from the data subjects.
- (b) Ping Identity will only Process or Transfer Personal Information as needed to provide the Services, as needed for its Internal Business Purposes, or in accordance with Customer’s documented instructions. This DPA, the Agreement, and Customer’s use of the Service’s features and functionality are Customer’s complete set of instructions to Ping Identity in relation to the processing of Personal Information. Ping Identity will promptly notify Customer if, in its opinion, the instructions given by Customer for Processing violate any Privacy Law; provided, however, that Ping Identity has no independent obligation to verify that the Processing complies with any specific Privacy Law, as it is entitled to rely on Customer’s instructions.
- (c) The Appendix below contains a general description of the Processing activities. Additional information about the Processing activities may be found in the Fact Sheets relevant to the Services that are posted in the Ping Identity Trust Center.
- (d) Unless otherwise prohibited by the Agreement or any applicable Privacy Law, Ping Identity may also further Process Personal Information as needed to Deidentify it and aggregate it with other customer or third-party data to create datasets for other appropriate internal operational purposes such as research, product development and analytics. To the extent these sets contain any unique record identifiers, indirect identifiers or otherwise continue to be regulated by the Privacy Laws, Ping Identity will comply with provisions of applicable Privacy Law and continue to handle the data in accordance with this DPA.
- (e) Ping Identity will promptly inform Customer in writing: (i) if it cannot comply with any material term of this DPA (if this occurs, Ping Identity will use reasonable efforts to remedy the non-compliance, and Customer will be entitled to suspend Ping Identity’s Processing of Personal Information); (ii) of any Data Subject Request received by it; (iii) of any other requests with respect to Personal Information received, including (without limitations) of any request for access to any Personal Information received by Ping Identity from any entity, including (without limitation) from any data protection agency, law enforcement agency or pursuant to any civil subpoena, unless it is explicitly prohibited by law from notifying Customer of the request. Ping Identity understands that it is not authorized with to respond to these requests without Customer’s approval unless the response is legally required under a subpoena or similar legal document issued by a government agency that

compels disclosure by Ping Identity.

- (f) Ping Identity will reasonably cooperate with Customer and with its Affiliates and representatives in responding to Data Subject Requests and regulatory inquiries as needed for Customer to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws. Ping Identity will reasonably assist Customer with any data protection impact assessments, transfer risk assessments or prior consultations with regulators as needed to comply with the Privacy Laws.

3. Specific Compliance Requirements. To the extent applicable:

- (a) Ping Identity certifies that it will not (i) sell the Personal Information or share the Personal Information with third parties for online targeting, (ii) retain, use or disclose the Personal Information other than as specified in the Agreement, as needed to perform the Services and for its Internal Business Purposes, (iii) retain, use or disclose the Personal Information outside of its direct business relationship with Customer.
- (b) If the Personal Information includes any Personal Information subject to the CA Privacy Laws, Ping Identity will comply with all applicable sections of the CA Privacy Laws, including by providing the same level of privacy protection as required by Customer. While not specifically incorporated by reference, Ping Identity is bound by all contract terms for service providers/contractors required by the Regulations implementing the CA Privacy Laws. More information about Ping Identity's commitment to CA Privacy Law compliance can be found in the Ping Identity Trust Center.
- (c) If the Personal Information includes EEA Personal Data, Ping Identity and Customer will ensure adequate protection for the EEA Personal Data. For any Restricted Transfers of EEA Personal Data, the parties will document adequate protection for the EEA Personal Data using an approved data transfer mechanism in accordance with Section 5 below. More information about Ping Identity's commitment to GDPR compliance can be found in the Ping Identity Trust Center.
- (d) If the Personal Information includes "protected health information" (PHI) as defined in the Privacy, Security and Breach Notification Rules issued under the Health Insurance Portability and Accountability Act ("HIPAA"), the parties agree that the Processing of all such PHI is subject to the existing Business Associate Agreement between Customer and Ping Identity.
- (e) If the Personal Information includes "consumer health data" as defined in an applicable Privacy Law or other sensitive Personal Information or special categories of data, the parties shall comply with the specific requirements for the Processing of these data elements. Ping Identity shall restrict access to these data elements to those personnel whose access is needed to provide the Services, and it shall only process these data elements in accordance with Customer's specific binding instructions. Ping Identity shall reasonably assist Customer as needed for Customer to comply with its obligations under applicable Privacy Laws that regulate these data elements.
- (f) Certain Ping Identity products and services incorporate AI Technology to improve usability, security, and fraud detection. Ping Identity uses reasonable and appropriate controls to manage its use of the AI Technology and validate that the outputs are free of inappropriate bias, given the purposes for which they are used.

4. Data Transfers and Subprocessors.

- (a) Ping Identity will only Transfer Personal information as authorized by Customer and permitted by applicable Privacy Laws. With respect to Ping Identity's hosted service, Customer may select the data center(s) location from those locations offered by Ping Identity in which Personal Information shall be physically stored. Customer understands and agrees that by instructing Ping Identity to use a Subprocessor (such as a data center), the Parties are bound by the Subprocessor's terms and conditions in addition to this DPA.
- (b) Customer authorizes Ping Identity to make routine Transfers of Personal Information in the normal course of business to itself in other countries and to its Affiliates, using intercompany contracts containing Standard Contractual Clauses or another approved mechanism. Ping Identity has certified to the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, and the UK Extension of the EU-US Data Privacy Frameworks. These certifications provide the primary authorization for Restricted Transfers of EEA Personal Data to Ping Identity in the United States.
- (c) Customer authorizes Ping Identity to Transfer Personal Information to the Subprocessors listed in the Ping Identity Data Supplement attached below as may be amended by Ping Identity from time to time and Customer may subscribe to receive updates from such website). In each case, Ping Identity: (i) has conducted adequate due diligence to verify that the Subprocessor is capable of providing the level of protection for Personal Information as is required by this DPA; (ii) will ensure that all Restricted Transfers of Personal Information to the Subprocessors are authorized using an approved

mechanism; (iii) has entered into a written contract with the Subprocessor that includes privacy and security terms no less stringent than are imposed on Ping Identity hereunder; and (iv) remains primarily liable to Customer for the acts, errors and omissions of the Subprocessor, as if they were Ping Identity's own acts, errors and omissions. Customer may at any time object to a Subprocessor for good cause by sending an email to legalnotice@pingidentity.com, and Ping Identity will not allow Subprocessor to Process any Personal Information until such objection is resolved. If the objection has not been resolved to the mutual satisfaction of the parties within thirty (30) days after Ping Identity's receipt of the objection, Customer may, as its sole and exclusive remedy, terminate its applicable subscriptions from Ping Identity with respect only to those aspects of the Service which cannot be provided by Ping Identity without the use of the new Subprocessor. In such event, Ping Identity shall refund Customer any unused, prepaid Fees for the applicable Service covering the remainder of the subscription term after the date of termination.

- (d) Should any supervisory authority or court determine that any Transfer mechanism used herein is no longer an appropriate basis for Restricted Transfers, Ping Identity and Customer will promptly take all steps reasonably necessary to demonstrate a adequate protection for the impacted information, using a nother approved mechanism. Ping Identity understands and agrees that Customer may terminate the Transfers as needed to comply with the applicable Privacy Laws.
- (e) Should other jurisdictions require specific contractual terms to enable Restricted Transfers, the parties will use good faith efforts to negotiate these instruments as needed to comply with the applicable Privacy Laws. If permitted by law, the parties agree that the terms of the new instruments will be automatically incorporated by reference into this DPA upon either party's circulation of an amendment containing the required transfer terms. The receiving party will have thirty (30) days to object to the amendment by giving the other party written notice, in which case Customer may terminate the Transfers as needed to comply with law.

5. Security and Personal Data Breaches.

- (a) Ping Identity has implemented and documented appropriate administrative, technical and physical measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access as described in more detail in the Ping Identity Security Exhibit attached hereto.
- (b) Ping Identity may disclose Personal Information to its employees and contingent workers as reasonably needed to provide the Services. Prior to allowing any employee or contingent worker to Process any Personal Information, Ping Identity shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (unless they are subject to a statutory or professional obligation of confidentiality), and (iii) provide the individual with appropriate privacy and security training. Ping Identity will also reasonably monitor its employees and contingent workers for compliance with the privacy and security program requirements.
- (c) Ping Identity will promptly investigate any security incident which is reasonably suspected to have resulted in the unauthorized access to, use or disclosure of the Personal Information. Ping Identity will notify Customer without undue delay upon determining that a Personal Information Breach impacts Personal Information. This notification will be made via email to the address specified by Customer in the Appendix. Ping Identity will provide Customer with all information in its possession about the Security Breach reasonably needed by Customer to assess its incident response obligations.
- (d) When the Ping Identity ceases to perform Services for Customer (and at any other time, upon request), Ping Identity will either (i) return the Personal Information or (ii) purge, delete and destroy the Personal Information. If Ping Identity is required by applicable law to retain any Personal Information, it shall (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed for to comply with law.

6. Audit.

- (a) Ping Identity and Customer will first use all reasonable efforts to satisfy Customer audit needs through (i) responses to a reasonable information security-related questionnaire; (ii) copies of Ping Identity's most recently completed SOC-2 Type II audit report, its public ISO 27001 certificate and non-public Statement of Applicability; (iii) a summary of Ping Identity's operational practices related to data protection and security; (iv) a summary of Ping Identity's operational practices related to data protection and security; (v) summary of the most recent annual penetration test; and (vi) making Ping Identity's personnel reasonably available for security-related discussions.
- (b) Where required by law, Ping Identity will submit its corporate headquarters for a reasonable audit upon at least 30 days prior written notice, not more than once per year, during Ping Identity's reasonable business hours, which shall be carried out by

Customer (or by a qualified independent auditor) in a mutually agreeable manner. In the event a Customer audit takes more than one business day, Customer shall reimburse Ping Identity for any time expended by Ping Identity in fulfilling any such request at Ping Identity's then-current professional services rates, which shall be made available to Customer upon request. Any independent auditors utilized shall be required to enter into a confidentiality agreement with Ping Identity. For the avoidance of doubt, Customer understands that due to the third-party hosting and multi-tenant nature of the Services, Ping Identity cannot grant access to the premises, facilities, or records of any Subprocessor or Ping Identity's production or non-production systems, source code, or anything that could expose sensitive information of Ping Identity or the confidential information of other customers of Ping Identity.

- (c) Ping Identity shall also cooperate with any audits conducted by any regulatory agency that has authority over Customer as needed to comply with applicable law.

7. Miscellaneous.

- (a) In the event of a conflict between the terms and conditions of the Subscription Agreement and this DPA, this DPA shall control.
- (b) This DPA shall remain in effect until, and automatically expire upon, deletion of all Personal Information by Ping Identity as described in this DPA.

Appendix to the Data Processing Addendum
This Appendix also serves as the Appendix to the Standard Contractual Clauses,
if those are used to authorize cross-border data transfers as indicated below.

ANNEX I

A. LIST OF PARTIES

Customer name and address as specified in the Agreement or above in this DPA.
Customer Contact for Breach Notification: [insert]
Customer acts as the data exporter/controller.

and

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202

Ping Identity acts as the data importer/processor, for itself and its Affiliates, as applicable.
Ping Identity Privacy Office: privacy@pingidentity.com

B. DESCRIPTION OF THE PROCESSING AND TRANSFER

Ping Identity provides enterprise identity and access management (IAM) products and related security solutions. Ping Identity's products enable customers to provide secure access to their networks and systems to their employees and customers. Ping Identity's products range from basic single sign-on solutions to fully orchestrated risk-based, adaptive authentication workflows that support different IAM use cases, such as fraud detection, identity proofing, and authorization.

Categories of data subjects whose personal data are processed and/or transferred

Customer's employees, users, and other persons whose information is processed by Ping Identity in the course of providing the IAM services to the Customer.

Categories of personal data are processed and/or transferred

- Contact information (such as name, address, email address)
- Professional details (such as employer, title, position)
- IAM data and technical information (such as access privileges and customer access criteria, access log information)
- Online and technical data (IP address, device ID and related data, connection data)
- For the PingOne Fraud Service: Behavioral characteristics (such as keystroke dynamics) which are used to detect bots and not used for individual identification.
- For the PingOne Da Vinci Service: The orchestration platform allows customers to process and store additional categories of data; these are determined by the customer and are not required by Ping Identity.

Sensitive data processed and/or transferred (if applicable)

Ping Identity's IAM products do not require sensitive data, but some products provide customers and end users with the capability to process biometric data for authentication and multi-factor authentication.

- *For the PingID Service:* The Service itself does not process biometric data but does allow users to authenticate using the biometric capabilities of their devices (such as TouchID).
- *For the PingOne Verify Service:* If implemented by customer, biometric data (facial recognition) is processed for authentication. The user uploads a photo to enable this functionality.
- *For the PingOne Da Vinci Service:* The orchestration platform allows customers to process and store additional categories of data, which may include special categories of data; these are determined by the customer and are not required by Ping Identity.

Nature of the processing

Personal data is processed for identity and access management in connection with the services set forth on the applicable Order Form. Ping Identity may further Process Personal Information for the following closely-related purposes: (i) detecting security incidents, and protecting against malicious, deceptive, fraudulent, or illegal activity; (ii) debugging to identify and repair errors that impair intended functionality of the Products and other activities needed to maintain the quality and/or safety of the products; and (iii) internal operational activities such as responding to data subject requests, making back-ups as part of disaster recovery/business continuity programs, confirming usage quantities, and processing required for legal or regulatory compliance.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained by the data importer in accordance with its data retention policy and no longer than necessary for the purposes set forth in the Agreement.

Physical location of the personal data

For hosted solutions, customer will select the data center(s) from those locations offered by Ping Identity.

Purpose(s) of the data transfer and further processing

To enable Ping Identity to provide the IAM products and services per the Agreement.

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

Continuous

C. COMPETENT SUPERVISORY AUTHORITY FOR RESTRICTED TRANSFERS

Restricted Transfer	Competent Supervisory Authority & Governing Law
EEA Transfers – per Schedule 1	Schleswig-Holstein DPA (Germany)
Swiss Transfers	Federal Data Protection & Information Commissioner (FDPIC) – Switzerland
UK Data Transfers – per Schedule 2	Information Commissioner (ICO) – United Kingdom

ANNEX II- TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Ping Identity’s information security program is described in Exhibit B and Exhibit C (as applicable)

ANNEX III – LIST OF SUBPROCESSORS

Customer has authorized Ping Identity’s use of the subprocessors found below,

PRODUCT-SPECIFIC SUB-PROCESSORS

Sub-Processor	Purpose of Processing	Location(s) of data centers	Data Processed for EEA, UK & Swiss customers?	Data stored outside the EU/ UK?	Product-specific sub-processor
Amazon Web Services (AWS)	Data center providing infrastructure-as-a-service, and email notification services for customers. Customers select the region(s) of data residency.	United States, Germany, Ireland, Australia, Canada, Singapore	Yes	Aligns with regions selected	PingOne Advanced Services may be deployed in other countries upon mutual agreement.
Amazon Web Services (AWS)	Rekognition image verification Data is stored in the region(s) selected by customer for PingOne tenant.	United States, Germany, Ireland, Australia, Canada, Singapore	Yes	Aligns with regions selected	PingOne Verify service only, when selected by customer.
DataZoo	Offering provides real-time identity verification by accessing authoritative sources.	United States, Canada, Australia, Singapore, Germany	Yes, PingOne Verify customers only.	Yes	PingOne Verify service only, when selected by customer.
Elasticsearch Inc	Visualization & Analytics	As configured by customer	Yes	Aligns with regions selected	IGA
Google Vertex AI	To provide generative artificial intelligence and natural language processing services to support technical troubleshooting and intelligent assistance.	Inference is co-located with the customer's deployment region	Yes	Inference is co-located with the customer's deployment region	Helix
IDLayr	Provides mobile-based identity verification using phone numbers as secure digital identities	United States, Germany	Yes	No	PingOne Verify service only, when selected by customer.
Mitek Systems	Document verification and image verification	United States, Ireland, Canada (only if configured by the customer)	Yes	Yes	PingOne Verify service only, when selected by customer.

MX Technologies	Authenticates account ownership through document-based verification.	United States	Yes, PingOne Verify customers only.	No	PingOne Verify service only, when selected by customer.
OpenAI	To provide generative artificial intelligence and natural language processing services to support technical troubleshooting and intelligent assistance.	Inference is co-located with the customer's deployment region	Yes	Inference is co-located with the customer's deployment region	Helix
Secret Double Octopus	Passwordless Authentication	Israel	Yes	Yes	Advanced IdentityCloud only
TransUnion	Verifying and processing biographic data and PII like address, name, SSN. Also verifying the identity associated with a payment card.	United States	Yes	Yes	PingOne Verify service only, when selected by customer.
Trinsic	Enables global interoperability of digital identities.	United States, India	Yes	Yes	PingOne Verify service only, when selected by customer.
Twilio	Secure SMS OTP and voice authentication	United States	Yes	Yes	PingID, PingOne MFA and PingOne Neo and Verify, when customer utilizes secure SMS service.
UberEther	FedRAMP infrastructure	United States	N/A	N/A	US FedRAMP customers only.
Veriff	Identification document verification	United States, Ireland	Yes	Yes	PingOne Verify service only, when selected by customer.
Vonage	Secure SMS authentication	United States	Yes	Yes	PingID and PingOne MFA, when customer utilizes secure SMS service.

OPERATIONAL SUB-PROCESSORS: INFRASTRUCTURE, MONITORING & SECURITY
Personal data processed in the ordinary course of operations

Sub-Processor	Description of Processing	Location(s) of data centers	Data Processed for EEA, UK & Swiss customers?	Data processed for non-US customers?
Amazon Web Services (AWS)	Data center providing infrastructure-as-a-service. Customers select the region(s) of data residency offered by Ping Identity.	United States, Germany, Ireland, Australia, Canada	Yes	Aligns with regions selected
Amazon Web Services (AWS)	Email notification services for customers. Customers select the region(s) of data residency offered by Ping Identity.	United States, Germany, Ireland, Australia	Yes	Aligns with regions selected
Cloudflare	<p>Cloudflare provides a content delivery network and distributed DOS attack prevention services, and offers security and performance benefits to all Ping cloud customers.</p> <p>Customers cannot select the region where data is processed.</p>	Cloudflare Network Locations	Yes	Yes
Google	<p>Corporate email and documentation.</p> <p>Email correspondence and documents may contain customer data.</p>	United States	Yes	Yes

Google	Hosting	As configured by customer	Yes	Aligns with Google regions selected
New Relic	Application performance management. Performance metrics for Customers' tenants.	United States	Yes, PingOne Verify customers only	Yes
Splunk	Operational logs and business analytics. Customer data is logged for event monitoring and troubleshooting purposes and is retained in the region of residency.	United States, Germany, Australia, Canada	Yes, PingOne Verify customers only	Aligns with AWS regions selected

OPERATIONAL SUB-PROCESSORS: CUSTOMER SUPPORT & INCIDENT RESPONSE				
Customer data processed only in the context of a customer support case or security incident				
Sub-Processor	Description of Processing	Location(s) of data centers	Data Processed for EEA, UK & Swiss customers?	Data stored outside the EU/UK?
Appfire	Salesforce-to-Jira integration Securely automates transfer of support ticket data from Salesforce to Jira.	United States	Yes	Yes
Atlassian Cloud	Documentation and issue tracking. Customer documentation and data related to support cases may be stored in Atlassian Cloud.	United States	Yes	Yes

Box	Storage and transfer of log files for customer support. Generally applicable when a customer files a support case and attaches customer data to the ticket (e.g., attachments, log files).	United States	Yes	Yes
Code42	Backup of customer support endpoints. Backup of customer support endpoints. Customer data related to support cases may be processed on endpoints in use by customer support personnel. All data is encrypted, and the encryption key is controlled by Ping.	United States	Yes	Yes
CrowdStrike	Incident response. CrowdStrike might have access to customer data in the event of a security incident.	United States	Yes	Yes
Glean	Glean provides AI-powered enterprise search and knowledge retrieval capabilities for workforce productivity.	United States	Yes	Yes
Google Chronicle	Security log and event management; security analytics. Customer data is logged for security monitoring and troubleshooting purposes.	United States	Yes	Yes
OwnBackup	Cloud backup of Salesforce data. When customers file a support case in Salesforce, that data will be backed up periodically.	United States	Yes	Yes

Salesforce	Service cloud that facilitates the customer support ticketing process. Customer data related to support cases may be stored in Salesforce.	United States	Yes	Yes
SupportLogic	Customer support case management Used to increase productivity and improve backlog management for the global customer support team.	United States	Yes	Yes

AFFILIATE SUB-PROCESSORS

Data processed for all products and customers, including non-US customers

Entity Name	Description of Processing	Location(s)
Ping Identity India Private Limited	Support and Operations	India
Ping Identity Australia Pty Ltd	Support and Operations	Australia
Ping Identity Canada Inc	Support and Operations	Canada
Ping Identity Israel Ltd.	Support and Operations	Israel
Ping Identity Singapore Pte. Ltd.	Support and Operations	Singapore
Ping Identity Corporation	Support and Operations	United States
Ping Identity Limited	Support and Operations	United Kingdom
ForgeRock AUS Pty. Ltd	Support and Operations	Australia

ForgeRock France SAS	Support and Operations	France
Ping Identity Deutschland GmbH	Support and Operations	Germany
Ping Identity NZ Limited	Support and Operations	New Zealand
Ping Identity AS	Support and Operations	Norway
Ping Identity France	Support and Operations	France