

FORTIOR PIV-I™ CUSTOMER AGREEMENT

Please carefully read the following terms and conditions of this Fortior PIV-I™ Customer Agreement (the “Agreement”). It is a legally binding contract and affects the legal rights of your company identified at the end of this Agreement.

By signing this Agreement below, and in consideration of the mutual covenants, terms and conditions described in this Agreement, you (1) certify that you have the authority to bind your company to the terms and conditions of this Agreement, (2) accept, on behalf of your company, the terms and conditions of this Agreement, and (3) agree, on behalf of your company, for your company to be bound by the terms and conditions of this Agreement.

Your company, referred to herein as “Customer”, enters into this Agreement with Fortior Solutions, LLC (“Fortior Solutions”), fka SureID, Inc. Fortior Solutions and Customer may be referred to herein as a “Party”, individually, and as the “Parties”, collectively.

- 1. Products.** All orders for and delivery of Fortior PIV-I™ Program (the “Program”) services, software, equipment and/or credentials (collectively the “Products”) are subject to the terms and conditions set forth in this Agreement.
- 2. Term and Termination.** The term of this Agreement (“Term”) begins on the Effective Date and will expire when Customer’s use of the Products ceases, unless earlier terminated as set forth in this Section. The Parties by mutual written agreement may terminate this Agreement prior to the expiration date. Further, either Party may terminate this Agreement due to the other Party’s material breach of this Agreement, if that breach is not cured within 10 days of written notice. Upon the expiration or termination of this Agreement, Customer must immediately cease use of the Products, and the digital certificates on any Program credentials that have been issued to any Customer Affiliate (as defined below) under the Program will be revoked.
- 3. Program Services and Software.**
 - 3.1.** The Program is designed to enhance identity management and security and to provide a means for authorized individuals to more quickly and securely access physical and logical systems, as well as to facilitate more secure email communication.
 - 3.2.** Program services includes the following:
 - 3.2.1.** An integrated, managed software-based Credential Management System and Identity Management System that support individual registration, credential issuance, and ongoing credential management
 - 3.2.2.** Registration of Customer Affiliates
 - 3.2.3.** Production, issuance, management, adjudication, and revocation of Program credentials and digital certificates
 - 3.2.4.** Maintenance and management of a Certification Authority (“CA”) that supports a trust relationship with the Federal Bridge Certification authority (“FBCA”). All Program credentials issued by/for Customer will be issued through this CA. Fortior Solutions will follow its Fortior Solutions TSCP PKI Credential Service Certificate Policy or its successor.
- 4. Program Equipment.**
 - 4.1.** Program equipment consists of Fortior PIV-I Registration Stations and Fortior PIV-I Issuance Stations, referred to collectively herein as “LRA Work Stations”. The LRA Work Stations will be furnished either as separate units or as a single integrated unit. Other Program equipment includes connection cables and power cords as needed. Program equipment is leased, not sold.
 - 4.2.** Fortior Solutions, its third-party service provider, or Customer will be responsible for installing Program equipment at Customer’s business premises, as determined by Fortior Solutions in its sole discretion. Customer acknowledges and agrees that the installation process may involve minor construction including securing the Program equipment to the premises. Fortior Solutions and its third-party service providers are not responsible for any incidental damage to Customer’s property arising from installation of the Registration Station.
 - 4.3.** Fortior Solutions or its third-party providers will provide routine maintenance of Program equipment at such times and with such frequency as determined by Fortior Solutions in its sole discretion. Fortior Solutions or its

third-party providers will perform any needed repairs of Program equipment. Customer shall notify Fortior Solutions within 24 hours of any needed repairs. Repairs will be performed at such times as determined by Fortior Solutions in its sole discretion. Customer is responsible for the costs of new equipment for replacement of lost or stolen equipment. Customer also is responsible for the costs of any repairs to equipment for damage beyond reasonable wear and tear. Neither Customer, nor anyone acting on behalf or at the behest of Customer, may perform any maintenance or repairs of Program equipment.

4.4. Physical and logical security requirements for Program equipment are set forth in Section 9.3 below.

5. Program Credentials.

- 5.1. Features.** Program credentials are Personal Identity Verification–Interoperable (“PIV-I”) credentials (“PIV-I Credentials”). PIV-I Credentials are secure identity credentials and contain four digital certificates that support physical access control, logical access control, encryption, and digital signatures. CUSTOMER MAY BE LIMITED IN ITS ABILITY TO USE THE FULL FORTIOR PIV-I CREDENTIAL FEATURES IF CUSTOMER AFFILIATES DO NOT PROVIDE A UNIQUE EMAIL ADDRESS DURING REGISTRATION OR DO NOT PROVIDE THE EMAIL ADDRESS OR USER PRINCIPAL NAME THAT CUSTOMER USES IN ITS ACTIVE DIRECTORY. Fortior PIV-I Credentials are the size of a common identification badge and display the individual’s name and photo, Customer name, and contain a unique ID.
- 5.2. Registration.** Only individuals who are affiliated with Customer through an employment relationship, independent contractor relationship, or other sponsored relationship (collectively “Customer Affiliates”) may register to receive a Fortior PIV-I Credential. Customer must designate an employee to be a Fortior PIV-I Company Administrator (“PCA”). The PCA must register for and receive a Fortior PIV-I Credential. The PCA is in charge of Customer’s internal Program administration and is responsible for managing the Fortior PIV-I Program Management Portal on behalf of Customer. Only the PCA may approve Customer Affiliates to receive a Fortior PIV-I Credential. Registration of Customer Affiliates involves the collection of certain biographic and biometric information as well as information validating affiliation and authorization to receive the Fortior PIV-I Credential. Customer Affiliates also will create their own unique Personal Identification Number (“PIN”), which Customer Affiliates must memorize in order to use their Fortior PIV-I Credential. Fortior Solutions has the right to charge Customer for the registration whether or not a Fortior PIV-I Credential ultimately is issued to the Customer Affiliate, unless non-issuance is due to the fault of Fortior Solutions.
- 5.3. Program Credential Printing and Issuance.** After a Customer Affiliate has registered for and is approved by the PCA for the Program, a Fortior PIV-I Credential is manufactured for and issued to the Customer Affiliate. A Customer Affiliate who is issued a Fortior PIV-I Credential is referred to as a “Subscriber”. The Subscriber must sign a Subscriber Agreement at the time of Fortior PIV-I Credential issuance. Issuance must be done according to Fortior PIV-I standards. These in-person issuances take place at (a) Customer facilities by Fortior Solutions employees or Fortior Solutions’ third-party Local Registration Authorities (“LRAs”), or (b) Fortior Solutions’ registration and issuance center at its Hillsboro, OR facility. (See Section 6, below, for information on issuances by Customer Employee PIV-I LRAs). The schedule for registration and issuance events will be mutually agreed upon in writing by Fortior Solutions and Customer. Fortior Solutions charges a fee to Customer for Fortior PIV-I issuance events.
- 5.4. Credential Issuance.** Fortior PIV-I Credentials must be issued by or for Customer within 60 days of shipping by Fortior Solutions. Customer is not entitled to a refund or credit for credentials that are not issued after this time. Customer must promptly destroy unissued Fortior PIV-I Credentials or securely return the credentials to Fortior Solutions.
- 5.5. Validity Period.** Fortior PIV-I Credentials are valid for three years from the date of issuance unless revoked earlier in accordance with this Agreement or the Subscriber Agreement.
- 5.6. Replacement Credentials; PIN resets.** Replacements of Fortior PIV-I Credentials (for example, if a credential is lost, stolen, or damaged, or if a Subscriber’s name changes, necessitating a new credential) can only be provided through in-person issuance. If Customer does not have a Customer Employee LRA (as defined below) and a Fortior PIV-I Issuance Station for in-person issuances, Customer will be charged the applicable Program credential replacement, Fortior PIV-I issuance event and related fees. The fees will apply regardless of the reason for replacement, including if the credential is damaged due to normal wear and tear. In addition, re-sets of PINS (for example, if a Subscriber forgets their PIN) can only be done through an in-person PIN re-set event. If Customer does not have a Customer Employee LRA and a Fortior PIV-I Issuance Station for PIN re-sets, Customer will be charged the applicable PIN re-set fees.

- 5.7. Customer Employee LRAs.** At the request of Customer, Fortior Solutions in its sole discretion may authorize Customer to nominate one or more Customer employees to serve as LRA's ("Customer Employee LRAs") to both register other Customer Affiliates for the Fortior PIV-I Program and to issue Fortior PIV-I Credentials to those Customer Affiliates. The following Fortior PIV-I requirements must be met.
- 5.8. Customer Employee LRA Eligibility Requirements.** Customer, through its PCA, may nominate one or more Customer employees to be appointed by Fortior Solutions to serve as a Customer Employee LRA. Fortior Solutions may appoint or reject a nominee, and may revoke its appointment of any Customer Employee LRA, in its sole discretion. All nominees must meet the following eligibility requirements:
- 5.8.1. Only current employees of Customer may serve as a Customer Employee LRA. Customer must immediately (a) initiate a request to Fortior Solutions to revoke the Fortior PIV-I Credential of a Customer Employee LRA, through the Fortior Solutions Program Management Portal, and (b) initiate a request to Fortior Solutions to deactivate the individual as a Company Employee LRA, through the Trusted Agent Management System Portal, when a Customer Employee LRA no longer is employed by Customer or for any other reason no longer is qualified or eligible to be a Customer Employee LRA.
- 5.8.2. Only Customer employees who have passed the Fortior Solutions-facilitated LRA background screenings may serve as a Customer Employee LRA. Customer will be charged the applicable processing fee(s) for the background screenings. The processing fee is non-refundable. The LRA background screenings may be conducted on a recurring basis. Customer will not receive a copy of LRA background screening reports or receive anything other than the pass/fail results of LRA background screenings. The LRA background screenings are conducted solely for the purpose of Fortior Solutions' evaluation of an individual's eligibility for appointment as an LRA. Such purposes may be considered "employment purposes" under applicable law. **HOWEVER, NOTWITHSTANDING THE FOREGOING, THE LRA BACKGROUND SCREENINGS ARE NOT CONDUCTED FOR CUSTOMER FOR PRE-EMPLOYMENT, EMPLOYMENT OR OTHER PURPOSES, AND CUSTOMER MAY NOT TAKE ADVERSE EMPLOYMENT ACTION AGAINST A CUSTOMER EMPLOYEE ON THE BASIS OF OR IN ANY WAY RELATING TO AN LRA BACKGROUND SCREENING OR LRA ELIGIBILITY DETERMINATION.** The specific LRA background screening elements may change from time to time but typically include a check for felonies and certain misdemeanors going back seven (7) years, verification of the individual's three (3) most recent employers during the last five (5) years, verification of the highest educational degree obtained, and a short interview with three (3) references in which the reference is asked whether he or she feels the LRA nominee is qualified to work on projects that require trustworthiness, integrity, and access to confidential information. Fortior Solutions may modify the background screening elements in its sole discretion.
- 5.8.3. Only Customer employees who have successfully completed Fortior Solutions' LRA training may serve as a Customer Employee LRA. This training may be provided via a combination of computer-based and in-person sessions.
- 5.8.4. Only Customer employees who have demonstrated to Fortior Solutions an ability to satisfactorily perform LRA duties may serve as a Customer Employee LRA.
- 5.8.5. Only Customer employees who have no duties that would interfere with their LRA duties may serve as a Customer Employee LRA.
- 5.8.6. Only Customer employees who are U.S. citizens may serve as a Customer Employee LRA.
- 5.9. Customer Employee LRA Operations.** Customer Employee LRAs must perform their duties in accordance with the training and instruction materials provided by Fortior Solutions.
- 5.10. Customer Employee LRA Workstation Security Requirements.**
- 5.10.1. Logical Security of Customer Employee LRA Workstation.**
- 5.10.1.1. Fortior Solutions will issue to each Customer Employee LRA a Fortior PIV-I credential, which the Customer Employee LRA must use to log into a Customer Employee LRA Workstation. Customer will be responsible for all associated Fortior PIV-I Credential fees.
- 5.10.1.2. Only a Customer Employee LRA who is logged into the Customer Employee LRA Workstation using their Fortior PIV-I Credential may operate or have access to a Customer

Employee LRA Workstation.

- 5.10.1.3. Customer Employee LRAs must keep their Fortior PIV-I Credential secure at all times and may not share their Fortior PIV-I Credential with anyone.
- 5.10.1.4. Customer Employee LRAs must keep the PIN for their Fortior PIV-I Credential secure at all times and may not share their PIN with anyone.
- 5.10.1.5. If a Customer Employee LRA's Fortior PIV-I Credential or PIN is lost, stolen, or compromised, (a) the Customer Employee LRA must immediately notify Customer's PCA, and (b) the Customer Employee LRA or the Customer PCA must immediately notify Fortior Solutions so that Fortior Solutions may revoke and disable the Fortior PIV-I Credential.
- 5.10.1.6. Customer may not install any software on a Customer Employee LRA Workstation.
- 5.10.1.7. Customer may not elevate any privileges on a Customer Employee LRA Workstation.
- 5.10.1.8. Customer may not access system resources or configuration of a Customer Employee LRA Workstation.
- 5.10.1.9. Customer may not plug-in or install any unauthorized hardware/peripherals on a Customer Employee LRA Workstation.
- 5.10.1.10. Customer may not repurpose any Customer Employee LRA Workstations.
- 5.10.1.11. Customer must keep Customer Employee LRA Workstations plugged in, turned on and connected to the Internet at all times, even when Customer Employee Workstations are not in use, so that data updates can be installed by Fortior Solutions. Customer will be responsible for paying Fortior Solutions for repair costs associated with any failure by Customer to meet this requirement.
- 5.10.1.12. Fortior Solutions retains the right to collect Customer Employee LRA Workstation log and system information at any time in its sole discretion.

5.10.2. Physical Security of the Customer Employee LRA Workstation.

- 5.10.2.1. The Customer Employee LRA Workstation must remain in its assigned secure location.
- 5.10.2.2. The Customer Employee LRA Workstation, its peripherals, and credential cardstock must be secured against theft and tampering when not in use.
- 5.10.2.3. The Customer Employee LRA Workstation must be protected from fire, water, and extreme temperature fluctuations.

6. Reliance upon Digital Certificates on Fortior PIV-I Credentials. Customer agrees that it will (i) use each digital certificate on a Fortior PIV-I Credential solely for the purpose for which it was issued, as indicated in the certificate information (i.e., the key usage extension); (ii) check each digital certificate on a Fortior PIV-I Credential for validity, prior to reliance; (iii) establish trust in the certificate authority that issued a certificate by verifying the certificate path; and (iv) if applicable, preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as necessary to verify the signature on that data.

7. Revocation of Digital Certificates on Program Credentials; Replacement Credentials; Collection of Program Credentials.

- 7.1. Customer's PCA must immediately initiate a revocation request to Fortior Solutions through the Fortior Solutions Program Management Portal, following which Fortior Solutions will revoke digital certificates on the Subscriber's Fortior PIV-I Credential, under any of the following circumstances: (i) a Subscriber no longer is affiliated with Customer; (ii) Customer discovers that a private key for a digital certificate on a Subscriber's

Fortior PIV-I Credential has been compromised or Customer suspects that the private key has been compromised; (iii) Customer discovers that a Subscriber's Fortior PIV-I Credential is lost, stolen, or damaged; (iv) Customer discovers that a Subscriber has violated the Subscriber Agreement (the Subscriber Agreement is posted at www.fortiorsolutions.com); (v) a Subscriber takes such actions as to call into question the Subscriber's trustworthiness as reasonably determined by the Customer; or (vii) Customer discovers that identifying information in the Subscriber's Fortior PIV-I Credential is or has become invalid.

- 7.2.** In addition to those circumstances described in the preceding subsection, Fortior Solutions has the right to revoke the digital certificates on a Subscriber's Fortior PIV-I Credential under the following circumstances: (i) following Fortior Solutions' discovery that the Subscriber has violated the Subscriber Agreement ; (ii) following the Subscriber's request that the certificates on his/her Fortior PIV-I Credential be revoked; (iii) following the Customer's failure to pay any amounts due; (iv) following Fortior Solutions' determination in its sole discretion that the "binding" status between the Subscriber and the public key within a digital certificate no longer is valid; or (v) following the termination or expiration of this Agreement.
- 7.3.** Revocation of a digital certificate is final and irreversible. A replacement digital certificate can only be provided through the issuance of a new Fortior PIV-I Credential at such prices as shall then be in effect. There is no proration, partial refund, or other credit for a Fortior PIV-I Credential on which the digital certificates have been revoked.
- 7.4.** If a Subscriber no longer is affiliated with Customer, or is otherwise disqualified to be an authorized Fortior PIV-I Credential holder, Customer must promptly collect the Fortior PIV-I Credential from that Subscriber and destroy the Fortior PIV-I Credential or securely return it to Fortior Solutions.
- 8. Encryption Key Recovery.** In the lifecycle of digital certificates it is common for Subscribers to use their encryption certificates to encrypt data or email. If a Subscriber ever is issued a replacement Fortior PIV-I Credential or other PIV-I Credential, or if there is some other event such as loss of affiliation, access to the encryption certificate that encrypted the original data may be lost. Fortior Solutions maintains copies of all private encryption keys. In cases where the Subscriber or Customer needs access to the archived private encryption keys, the keys may be recovered in accordance with Fortior Solutions' key recovery policies and practices.
- 9. Intellectual Property.** Fortior Solutions reserves all rights, title and interest in and to the Products provided under this Agreement, including all Intellectual Property rights. No Intellectual Property Rights are granted to Customer under this Agreement except as may be expressly set forth herein. As used herein, Intellectual Property Rights means any and all rights existing under patent law, copyright law, moral rights law, trade secret law, trademark law, unfair competition law, publicity rights law, privacy rights law, and any and all other proprietary rights, and any and all applications, renewals, extensions and restorations thereof, now or hereafter in force and effect worldwide.
- 10. Data.** Fortior Solutions will use personally identifiable information ("PII") collected or generated by the Program only in connection with the Program, except to the extent necessary to comply with legal requirements. Fortior Solutions may share PII with its third-party providers in connection with the Program. Fortior Solutions will not sell or rent PII to any third parties. Fortior Solutions will use commercially reasonable means to protect all PII in its possession.
- 11. Title in All Property.** Fortior Solutions retains all rights, title and interest in all Program services, software and equipment it furnishes for use by Customer. Customer may use the Program services, software, equipment and credentials solely for the purposes described in this Agreement.
- 12. Limited Warranty.** Fortior Solutions will perform services in a good and workmanlike manner, pursuant to applicable laws and regulations and generally accepted industry standards. All furnished equipment, software, equipment and credentials will be free of material defects under normal use and service; provided, however, that (A) CERTIFICATES ISSUED BY FORTIOR SOLUTIONS AND THE FORTIOR SOLUTIONS PKI ARE PROVIDED "AS IS", AND FORTIOR SOLUTIONS, ITS EMPLOYEES, OFFICERS, DIRECTORS, AGENTS, CONTRACTORS, ASSIGNS, REPRESENTATIVES, AND AFFILIATES DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, LACK OF REASONABLE CARE, OR THAT THE PRODUCTS WILL BE ERROR FREE OR COMPLETELY SECURE, AND (B) THE ENTIRE RISK OF THE USE OF FORTIOR PIV-I CREDENTIALS AND CERTIFICATES, THE USE OF PROGRAM SERVICES, SOFTWARE AND EQUIPMENT, AND THE VALIDATION OF ANY DIGITAL SIGNATURES, LIES WITH CUSTOMER.

- 13. Use of Products.** Customer may not use the Products for any unlawful or unauthorized purposes and must comply with all applicable laws and regulations.
- 14. Limitation of Liability.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, FORTIOR SOLUTIONS (INCLUDING, BUT NOT LIMITED TO, ITS RELATED COMPANIES, OFFICERS, DIRECTORS, MANAGERS, EMPLOYEES, AGENTS, CONTRACTORS, THIRD-PARTY SUPPLIERS, ASSIGNS, SUCCESSORS, REPRESENTATIVES, AND OTHER AFFILIATES (COLLECTIVELY, "FORTIOR SOLUTIONS RELATED PARTIES") (A) SHALL NOT BE LIABLE FOR ANY INDIRECT DAMAGES, CONSEQUENTIAL DAMAGES, INCIDENTAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR CUSTOMER'S USE OF ANY PRODUCT INCLUDING SERVICES, SOFTWARE, EQUIPMENT AND CREDENTIALS, EVEN IF FORTIOR SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, (B) SHALL NOT BE LIABLE FOR ANY USAGE OF A CERTIFICATE THAT FAILS TO CONFORM TO THE APPLICABLE LIMITATIONS OF USAGE, (C) SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER'S PRIVATE KEY OR ANY LOSS OF DATA. THE MAXIMUM LIABILITY OF FORTIOR SOLUTIONS AND THE FORTIOR SOLUTIONS RELATED PARTIES TO CUSTOMER UNDER OR RELATING TO THIS AGREEMENT SHALL BE EXCLUSIVELY LIMITED TO (i) DIRECT DAMAGES DIRECTLY RESULTING FROM FORTIOR SOLUTIONS' GROSS NEGLIGENCE OR WILLFUL MISCONDUCT IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT AND (ii) SHALL NOT EXCEED ONE THOUSAND DOLLARS (\$1,000) PER TRANSACTION (WHERE "TRANSACTION" MEANS WHEN A RELYING PARTY (INCLUDING CUSTOMER) RELIES UPON A PROGRAM CREDENTIAL AND TAKES OR ALLOWS AN ACTION OR SERIES OF ACTIONS AS A CONSEQUENCE OF SUCH RELIANCE) AND TEN THOUSAND DOLLARS (\$10,000) IN THE AGGREGATE.

CUSTOMER ACKNOWLEDGES THAT FORTIOR SOLUTIONS AND THE FORTIOR SOLUTIONS RELATED PARTIES HAVE NO RESPONSIBILITY OR LIABILITY FOR USE (OR MISUSE) OF A CUSTOMER AFFILIATE'S FORTIOR PIV-I CREDENTIAL. ALL ACCESS DECISIONS RELATING TO CUSTOMER'S OR A THIRD PARTY'S FACILITIES AND SYSTEMS ARE CUSTOMER'S SOLE RESPONSIBILITY, AND FORTIOR SOLUTIONS AND THE FORTIOR SOLUTIONS RELATED PARTIES DISCLAIM ALL RESPONSIBILITY AND LIABILITY THEREFOR.

- 15. Indemnification.** Products are provided as tools to enhance identity management and physical and logical access control. Customer hereby agrees to defend, indemnify, and hold harmless Fortior Solutions and the Fortior Solutions Related Parties, of and from any and all damages, losses, liabilities, taxes, assessments, fines, penalties, judgments, awards, costs, and expenses, including but not limited to reasonable attorneys' fees (collectively "Losses") arising out of or relating to any claim, allegation, action, suit, proceeding, demand or dispute (collectively "Dispute") brought by any third party relating in any way to Customer's use of Services or breach of this Agreement, including but not limited to access/entry related decisions or actions by Customer, and any other use of Fortior PIV-I credentials by a Customer Affiliate. Notwithstanding anything to the contrary in this section, Customer's indemnification obligations do not extend to Disputes involving allegations that Fortior Solutions has violated the intellectual property rights of third parties.
- 16. Governing Law; Arbitration; Jurisdiction; Class Action Waiver.** This Agreement is governed by, and construed and enforced in accordance with, the internal laws of the State of Oregon applicable to contracts made and to be wholly performed within Oregon by persons domiciled in Oregon, without reference to Oregon conflicts of law provisions. With respect to the breach or interpretation of this Agreement or the enforcement of any and all rights, duties, liabilities, obligations, powers, and other relations between the Parties arising under or relating to this Agreement, the Parties agree that their sole legal remedy is to refer such matters to binding arbitration before a single arbitrator pursuant to the rules of the American Arbitration Association or such other arbitration rules as the Parties mutually agree to in writing. The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve any dispute relating to the interpretation, applicability, enforceability or formation of this Agreement including, but not limited to, any claim that all or any part of this Agreement is void or voidable. Unless otherwise required by applicable law, each Party shall bear its own costs and attorneys' fees without regard to which Party is deemed to be the prevailing party in the arbitration proceeding. The arbitrator shall otherwise be authorized to award either Party any remedy permitted by applicable law. All arbitration proceedings arising hereunder, and any judicial actions brought to enforce an arbitrator's award or otherwise arising from or relating to this Agreement, must be brought and maintained in Washington County or Multnomah County, Oregon, and in the event of any judicial action the Parties agree to submit to the exclusive jurisdiction and venue of the state and federal courts sitting in Washington County or Multnomah County, Oregon, therefor. ANY DISPUTE RESOLUTION PROCEEDINGS, WHETHER IN ARBITRATION OR COURT, WILL BE CONDUCTED ONLY ON AN INDIVIDUAL BASIS AND NOT IN A CLASS OR REPRESENTATIVE ACTION OR AS A NAMED OR UNNAMED MEMBER IN A CLASS, CONSOLIDATED, REPRESENTATIVE OR PRIVATE ATTORNEY GENERAL ACTION, UNLESS BOTH CUSTOMER AND FORTIOR SOLUTIONS SPECIFICALLY AGREE IN WRITING TO THE CONTRARY FOLLOWING INITIATION OF THE ARBITRATION.



- 17. **Severability.** If any provision of this Agreement is held to be invalid or unenforceable to any extent, the Agreement will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Agreement will not be affected.
- 18. **Notices.** All notices under this Agreement will be deemed effective if given in writing and delivered in person, transmitted by fax, transmitted by overnight delivery by a nationally recognized service, or mailed, properly addressed and stamped with the required postage to the signatory for the Party receiving the notice. Notices will be deemed effective on the earlier of actual receipt or three (3) business days after mailing. Notices to Fortior Solutions shall be given to Legal Department, Fortior Solutions, LLC, 5800 NE Pinefarm Court, Hillsboro, OR 97124. Notices to Customer shall be given to the address listed by Customer at the end of this Agreement.
- 19. **Force Majeure.** Each Party will be excused from performance, other than payment obligations, for any period during which, and to the extent that, it is prevented from performing any obligation or service, in whole or in part, due to unforeseen circumstances or to causes beyond such Party's reasonable control including but not limited to war, strike, riot, telecommunication or Internet outages, cybersecurity incidents, failure of any transportation or communication system, loss (including but not limited to loss of a certificate authority or loss of authorizations needed to provide any Products), acts or omissions of suppliers or other causes beyond the Party's control, loss of a certificate authority, loss of authorizations needed to provide any Products, labor disputes, crime, acts of God, Government action, acts of terrorism, or shortages of resources.
- 20. **Assignments.** Customer may not assign this Agreement without the prior written consent of Fortior Solutions, except that Customer may assign the Agreement in connection with a sale of all or substantially all Customer's assets, so long as the assignment is to the acquirer of such assets.
- 21. **No Third Party Beneficiaries.** Nothing in this Agreement, express or implied (except for those sections pertaining to the Fortior Solutions Related Parties), is intended to or shall confer upon any other person any right, benefit or remedy of any nature whatsoever in connection with this Agreement.
- 22. **Use of Third Parties.** Fortior Solutions may contract with third-party providers to assist in Fortior Solutions' provision, support, or performance of the Products.
- 23. **Survival of Terms.** Any term of this Agreement that should be reasonably expected to survive expiration or termination of this Agreement will survive, including, but not limited to, confidentiality, restrictions on use of intellectual property, indemnity obligations, limitations on liability and disclaimers of warranties and damages, governing law, arbitration, and Customer's payment obligations accrued prior to termination or expiration.
- 24. **Headings.** Headings in this Agreement are for convenience of reference only and may not be interpreted to limit or otherwise affect the provisions of this Agreement.
- 25. **Entire Agreement; Modifications.** This Agreement constitutes the entire agreement between the Parties with respect to the subject matters herein and merges all prior and contemporaneous communications and proposals, whether electronic, oral or written, between the Parties with respect to such subject matters. Fortior Solutions may amend or modify this Agreement at any time. Fortior Solutions with written notification to Customer. The amended or modified Agreement will become binding on Customer 10 (ten) days after notification.

I hereby (1) certify that I have the authority to bind Customer to the terms and conditions of this Agreement, (2) accept, on behalf of Customer, the terms and conditions of this Agreement, and (3) agree, on behalf of Customer, for Customer to be bound by the terms and conditions of this Agreement.

Name (Signed)

Name of Customer

Name (Printed)

Customer Address (line 1)

Title

Customer Address (line 2)

Date

Customer Address (line 3)