Identity as a Service

Terms Of Service

The Agreement for Entrust's Identity as a Service Offering ("IDaaS") is made up of these terms of service (the "IDaaS Schedule"), the Entrust General Terms and Conditions ("General Terms") available at https://www.entrust.com/general-terms.pdf, and an Order for IDaaS. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. Definitions. The following capitalized terms have the meanings set forth below whenever used in this IDaaS Schedule.

1.1. "Authentication Record" means a record setting out the details of each authentication attempt made by a User. Authentication Records may include Personal Data.

1.2. "AUP" means the Entrust acceptable use policy for the Hosted Service, as may be modified from time to time, available at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/identity-as-a-service-acceptable-use-policy.pdf.

1.3. "Customer Account" means the account Customer sets up through the Hosted Service once Customer has agreed to the terms and conditions of the Agreement, including any subordinate accounts.

1.4. "Customer Data" means any data, or information that is supplied to Entrust on Customer's behalf, through the Customer Account or otherwise in connection with Customer's or its Users' use of the Entrust Technology (including, without limitation, device, and computer information). Customer Data may include Personal Data, but excludes Service Data, Profile data, Customer Confidential Information and Excluded Data.

1.5. "Customer Systems" means computer systems or networks under the ownership, possession, or control of Customer, for which the Hosted Service is being used to authenticate Users' access.

1.6. "Documentation" means written materials prepared by Entrust (or its licensors or service providers) relating to the Entrust Technology, including, without limitation, guides, manuals, instructions, policies, reference materials, professional services bundle descriptions, release notes, online help or tutorial files, support communications (including any disputes between the parties) or any other materials provided in connection with modifications, corrections, or enhancements to the Entrust Technology, all as may be modified from time to time.

1.7. "Entrust Technology" means the Hosted Service, the Software, the Tokens, and the Documentation.

1.8. "Extension" means an Entrust suite, configuration file, add-on, software integration, technical add-on, example module, command, function, or application separately licensed by Entrust to Customer, that extends the features or functionality of third-party software or services separately licensed or lawfully accessed by Customer.

1.9. "Hosted Service" means, in this IDaaS Schedule, the Identity as a Service cloud-based offering.

1.10. "Profile" means User and device profiles constructed from authentication patterns and device-identifying technical data. Profiles may include data from third party service providers and may also include Personal Data.

1.11. "Service Data" means any information and data relating to the access, use, and/or performance of the Entrust Technology, including data generated in connection with Customer's and/or Users' use of the Entrust Technology (e.g., analytics data, statistics data, and performance data). Service Data does not include Authentication Records, Customer Data, Profiles, or Personal Data.

1.12. "SLA" means Entrust's standard service level agreement for the Hosted Service, as may be modified from time to time, available at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/identity-as-a-service-service-level-agreement.pdf.

1.13. "Software" has the meaning set out in the General Terms, and in this IDaaS Schedule includes the Entrust Identity as a Service Gateway software application, and any updates, new versions, or replacement versions Entrust provides to Customer, as applicable.

1.14. "Special Terms and Conditions" means any terms and conditions attached to this IDaaS Schedule.

1.15. "Tokens" means the tokens (if any) specified in the Order.

1.16. "Third-Party Integrations" has the meaning set out in Section 5.7 (*Third-Party Integrations*).

1.17. "User" has the meaning set out in the General Terms, and in this IDaaS Schedule includes any individual end user who accesses or uses the Hosted Service through the Customer Account via the Hosted Service portal or otherwise (e.g. API-based access).

2. Hosted Service; Software.

2.1. Hosted Service. Customer receives no rights to the Hosted Service other than those specifically granted in Section 2.1 (Hosted Service).

2.1.1. Right to Access and Use. Subject to Customer's compliance with the Agreement, Entrust grants Customer, during the Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service: (i) via the Hosted Service portal or otherwise (ii) in accordance with the AUP; (iii) in accordance with the Documentation; (iv) in accordance with any specifications or limitations set out in the Order or imposed by technological means of the capabilities of the Hosted Service that Customer is permitted to use, such as limits associated with number of Users, or bundle entitlements, etc.; and (v) for the sole purpose of authenticating the identity of Users.

2.1.2. Licenses from Customer. Customer grants to Entrust a non-exclusive, nontransferable worldwide right to copy, store, record, transmit, display, view, print or otherwise use any trademarks that Customer provides Entrust for the purpose of including them in Customer's user interface of the Hosted Service ("Customer Trademarks").

2.1.3. Service Levels. The sole remedies for any failure of the Hosted Service are listed in the SLA. Service credits issued pursuant to the SLA, if any, will only be applied against the costs

associated with Customer's subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

2.1.4. Service Revisions. Entrust may modify or eliminate Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to the Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice at the Hosted Service portal constitutes written notice).

2.1.5. Users; Configuration and Security Measures. Customer is responsible and liable for any and all acts and/or omissions of its Users in relation to or breach of the Agreement or otherwise in relation to Users' access to and use of the Hosted Service. Customer will (i) only permit Users access to and use of the Hosted Service in combination with Customer's products or systems; (ii) prohibit any User from decompiling, reverse engineering or modifying the Hosted Service (except as and only to the extent any foregoing restriction is prohibited by applicable laws, rules, or regulations); (iii) make no representations or warranties regarding the Hosted Service to Users for or on behalf of Entrust; (iv) not create or purport to create any obligations or liabilities on or for Entrust regarding the Hosted Service. Customer is also responsible and liable for: (a) account usernames, passwords and access tokens; (b) the configuration of the Entrust Technology to meet its own and its Users' requirements; (c) Customer Data, Profiles, Personal Data, and any other data uploaded to the Hosted Service through the Customer Account or otherwise by Customer or its Users; (d) Customer's or its Users' access to and use of the Hosted Service; (e) any access to and use of the Hosted Service through the Customer Account; and (f) maintaining adequate security measures and the legally required protection for Customer Systems and data in Customer's possession or control or data otherwise residing on Customer Systems.

2.2. Software. If Entrust provides any Software in connection with the Hosted Service, the Schedule provided with the Software will apply (and not this IDaaS Schedule). If no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license available at https://www.entrust.com/end-user-license.pdf.

2.3. Documentation. Customer may use the Documentation solely as necessary to support Customer's access to and use of the Entrust Technology. Each permitted copy of all or part of the Documentation must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust or downloaded or otherwise accessed by Customer.

2.4. Support. Entrust provides the support commitments set out in the Support Schedule available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf for the Hosted Service. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to the Hosted Service. Other levels of Support may be available for purchase for an additional fee.

2.5. Professional Services. Entrust may provide set-up support and/or other Professional Services for some deployments of the Hosted Service, as specified in an Order, in which case the Professional Services will be provided in accordance with the applicable Order, the General Terms, and, if applicable, a Schedule describing the bundle of Professional Services purchased.

2.6. Unauthorized Access. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Entrust Technology or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

3. Evaluation; NFR.

3.1. Evaluation Purposes. Entrust may grant Customer the right to download, install, access, and use the Entrust Technology for evaluation purposes for the Trial Period. During the Trial Period Customer may not (i) use the Entrust Technology in order for Customer to generate revenue; or (ii) use any Customer Data or Personal Data in its evaluation of the Entrust Technology - only fictitious non-production data can be used.

3.2. Not-for-Resale (NFR) Purposes. Entrust may grant Customer the right to download, install, access, and use the Entrust Technology for not-for-resale (NFR) purposes for the NFR Period. NFR rights are granted to Customers that are Entrust authorized distributors, resellers, or indirect resellers (for the purposes of this Section, "Authorized Resellers"). During the NFR Period Authorized Reseller may download, install, access, and use the Entrust Technology for purposes of development, testing, support, integration, proofs of concept and demonstrations. Customer shall not use any Customer Data or Personal Data in its NFR use of the Entrust Technology other than Customer Data or Personal Data that is from its own personnel (i.e. not that of prospective clients) or other third parties.

3.3. Inapplicable Sections. Section 2.1.3 (*Service Levels*) does not apply to Customer's download, installation, access, or use of the Entrust Technology for evaluation or NFR purposes.

3.4. Trial Period. Customer's evaluation of the Hosted Service pursuant to this Section 3 (*Evaluation; NFR*) shall commence upon Customer's acceptance of the Agreement and continue for a period of thirty (30) days ("Trial Period"), or as otherwise agreed to by Entrust in writing with Customer.

3.5. NFR Period. Customer's access to and use of the Entrust Technology for NFR purposes pursuant to this Section 3 (*Evaluation; NFR*) shall commence on Customer's acceptance of the Agreement and continue for the duration indicated in the Order or the Documentation ("NFR Period").

3.6. Termination or Suspension. Notwithstanding the foregoing, Entrust may in its sole discretion suspend or terminate Customer's evaluation or NFR access to and use of, the Entrust Technology at any time, for any or no reason, without advanced notice.

4. Fees. Customer will pay the costs and fees for the Entrust Technology as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

5. Data and Privacy.

5.1. Customer Data; Profiles; Authentication Records; Personal Data. Customer acknowledges and agrees that the Entrust Technology requires certain Customer Data, Profiles, and Personal Data, in order to operate. Use of the Entrust Technology by Customer and Users will also generate Authentication Records. Customer grants to Entrust, its Affiliates, and any of their respective applicable subcontractors and hosting providers, a world-wide, limited right, during the Term, to host, copy, store, transmit, display, view, print or otherwise use Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide the Entrust Technology in accordance with the Agreement.

5.2. Cloud Risks & Data Safeguards. Customer understands that the Hosted Service is a cloud-hosted service. Although Customer Data may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Hosted Service, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Customer Data or any data stored in, transferred to or from, or otherwise processed by the Hosted Service, including in

transit. Customer is responsible for determining whether the Hosted Service offers appropriate safeguards for Customer's intended use of the Hosted Service, including any safeguards required by applicable laws, prior to transmitting or processing, or prior to permitting Users to transmit or process, any data or communications via the Hosted Service.

5.3. Profiles; Service Data; Use of Data. Entrust owns all right, title and interest in and to Service Data and Profiles (excluding any Personal Data contained in the Profiles) and, without limiting the generality of the foregoing, may use, reproduce, sell, publicize, or otherwise exploit such Profiles and Service Data in any way, in its sole discretion.

5.4. Consents. Customer represents and warrants that, before authorizing a User to use the Entrust Technology and before providing Customer Data or Personal Data to Entrust, Customer will have obtained from Users the requisite consents (if any) or satisfied other legal basis of processing Personal Data, and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data, by Entrust (including by any of its applicable subcontractors or hosting service providers) in accordance with the Agreement. Customer hereby grants Entrust (including any of its applicable Affiliates, subcontractors, or hosting service providers) all rights and consents required for the collection, use, and disclosure of the Customer Data in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Customer Content and the means by which Customer acquired them.

5.5. Consents Relating to Extensions. Customer acknowledges and agrees that certain Extensions may enable third-party software or third-party services (including cloud services) to download certain Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data from the Entrust Technology, and, by enabling such third-party software or third-party services (including cloud services) Customer agrees to such downloads. Customer represents and warrants that, before using any Extension, Customer will have obtained from Users the requisite consents (if any) or satisfied other legal basis of processing Personal Data, and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations in order to allow for the downloading and/or transfer of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, from Entrust (including any applicable subcontractors and hosting providers) to the Customer-licensed third-party software or third-party services (including cloud services) enabled by the Extension.

5.6. Consents Relating to Third-Party Service Providers. Customer consents to and represents and warrants that it will obtain all Users' consents necessary for, Entrust's use of third-party service providers, including, without limitation, hosting providers (who may further utilize subcontractors) in the provision of the Hosted Service. Customer acknowledges and agrees that Authentication Records, Customer Data, Profiles, Personal Data, and Service Data, may be transmitted to, processed by and/or reside on computers operated by the Entrust authorized third parties (e.g. Entrust's hosting providers) who perform services for Entrust. These third parties may use or disclose such Authentication Records, Customer Data, Profiles, Personal Data, and Service Data to perform the Hosted Service on Entrust's behalf or comply with legal obligations. Unless otherwise required by applicable laws, rules or regulations, and without limiting the generality of Section 11 (*Liability*) of the General Terms, Entrust shall have no responsibility or liability for Customer's failure to obtain any of the consents or disclosures described in this Section (*Consents Relating to Third-Party Service Providers*).

5.7. Third-Party Integrations. Customer may enable integrations between the Entrust Technology and certain third-party services contracted by Customer (each, a "Third-Party Integration"). By enabling a Third-Party Integration between the Entrust Technology and any such third-party services, Customer is expressly instructing Entrust to share all Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, necessary to facilitate the Third-Party Integration. Customer is responsible for providing any and all instructions to such third party

services provider about the use and protection of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data. Customer acknowledges and agrees that Entrust is not a sub-processor for any such third-party services providers in relation to any Personal Data contained in the aforementioned data or information, nor are any such third-party services providers sub-processors of Entrust in relation to any Personal Data contained in the aforementioned data or information.

5.8. Face Biometric Authenticator. To the extent Customer selects the face biometric authenticator within the Hosted Service, the use of such authenticator is governed by a separate agreement entered into between Customer and Onfido (an Entrust Affiliate)(the "Onfido Services Agreement") and Customer is solely responsible for ensuring its use of the face biometric authenticator complies with the Onfido Services Agreement.

5.9. Data Accuracy. Entrust will have no responsibility or liability for the accuracy of data uploaded to the Hosted Service by Customer or its Users, including, without limitation, Customer Data, Profiles, and Personal Data. Customer shall be solely responsible for the accuracy, quality, integrity, and legality of Customer Data or Personal Data and the means by which Customer acquired them.

6. Feedback.

6.1. Feedback. "Feedback" refers to Customer's suggestions, comments, or other feedback about the Entrust Technology or other Entrust products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust. Customer hereby agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer's right, title, and interest thereto, including without limitation intellectual property rights.

7. Warranty Disclaimers.

7.1. Warranty Disclaimers. For the purposes of this IDaaS Schedule, the following is added to the disclaimer of warranties in the General Terms: Entrust makes no representations, conditions or warranties: (i) that the Entrust Technology will be free of harmful components; (ii) that Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data or any other Customer content or data stored in, transferred to or from, or otherwise processed by the Entrust Technology, including in transit, will not be damaged, stolen, accessed without authorization, compromised, altered, or lost.

8. Indemnities.

8.1. In addition to the indemnification obligations in the General Terms, Customer agrees to defend, indemnify and hold harmless Entrust, its Affiliates and licensors, and each of their respective employees, officers, directors, and representatives against any and all third party claims, demands, suits or proceedings, fines, costs, damages, losses, settlement fees, and expenses (including investigation costs and attorney fees and disbursements) arising out of or related to: (i) Customer's breach of Section 5 (*Data and Privacy*); (ii) the Customer Data, Personal Data, or Excluded Data provided by the Customer or its Users; (iii) an allegation that the Customer Data, including written material, images, logos or other content uploaded to the Entrust Technology through the Customer Account, infringes or misappropriates a third party's intellectual property rights; (iv) a dispute between Customer and any User, or a claim by a User; (v) the injury to or death of any individual, or any loss of or damage to real or tangible personal property, caused by the act or omission of Customer; or (vi) Customer use of the Entrust Technology in breach of 3.1 (*Evaluation Purposes*), or 3.2 (*Not-For-Resale* (*NFR) Purposes*) (each of (i)-(vi), an additional "Customer Indemnified Claim" as such term is used in the General Terms).

9. Term, Termination and Suspension.

9.1. Term. The Hosted Service is sold on a subscription basis. Unless otherwise specified on the Order, the Offering Term for the Hosted Service will commence on the date that the Order is accepted by Entrust and will continue in effect for the period specified in the Order (or until the date the Trial Period or NFR Period expires), unless terminated in accordance with the Agreement.

9.2. Termination. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement for the Hosted Service (i) if Customer commits a material breach of this IDaaS Schedule and fails to remedy such material breach within 30 days (or such longer period as Entrust may approve in writing) after delivery of the breach notice; and (ii) for any reason by providing Customer advance notice of at least 1 year, unless Entrust discontinues the general commercial availability of the Hosted Service, in which case Entrust may terminate the Agreement upon 180 days' notice to Customer.

9.3. Termination or Suspension by Entrust. Entrust may, at its sole discretion, suspend or terminate Customer's or its Users' access to the Entrust Technology at any time, without advanced notice, if: (i) Entrust reasonably concludes that Customer or its Users' have conducted themselves in a way (a) that is not consistent with or violates the requirements of the AUP, the Documentation, or is otherwise in breach of the Agreement; or (b) in a way that subjects Entrust to potential liability or interferes with the use of the Entrust Technology by other Entrust customers or users; (ii) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' or users' information or data processed by the Entrust Technology; or (iii) Entrust reasonably concludes that Customer or Users are violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's or User's access to the Entrust Technology for scheduled or emergency maintenance. Termination of the Agreement will result in termination of all Orders.

9.4. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination or expiration of the Hosted Service, Entrust will have no further obligation to provide the Entrust Technology, Customer will immediately cease all use of the Entrust Technology, and Customer will return all copies of Confidential Information to Discloser or certify, in writing, the destruction thereof, destroy any copies of Documentation, and delete any Software in its possession or control. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (*Effects of Termination*), confidentiality, disclaimers, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed. Termination or expiration (non-renewal) of the Agreement also terminates all Special Terms and Conditions and the parties' ability to enter into any new Orders (including Orders to renew). Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Termination will not relieve Customer (directly or through an authorized reseller) from any obligation to pay Entrust any and all fees or other amounts due under the Agreement.

10. Open Source Software and Third Party Products.

10.1. Open Source. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("**Ancillary Software**"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

10.2. Third Party Products and Services. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in

connection with the Hosted Services ("**Third Party Vendor Products**"). Except as expressly stated in this IDaaS Schedule, Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the third party vendor's terms, conditions and policy documents ("**Vendor Terms**") accompanying, embedded in, or delivered with the Third Party Vendor Products, or otherwise made available by the third party vendor.

11. Miscellaneous.

11.1. Order of Precedence. In the event of a conflict or differences between this IDaaS Schedule and Special Terms and Conditions, the Special Terms and Conditions will prevail over any conflicting provisions.

11.2. Publicity. Customer agrees to participate in Entrust's press announcements, case studies, trade shows, or other marketing reasonably requested by Entrust. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name and/or logo, worldwide, to identify Customer as such on Entrust's website or other marketing or advertising materials.

11.3. Extensions and Third-Party Integrations. Customer's use of any Extension shall be subject to a separate end user license agreement (or other applicable agreement) between Customer and Entrust (or one of its Affiliates). Customer's use of any Third-Party Integration shall be subject to the separate end user license agreement (or other applicable agreement) between Customer with the relevant third party (e.g. service provider that provides the service which is the subject of the Third-Party Integration).

11.4. Tokens. If an Order calls for Tokens (or if Customer purchases Tokens through an Authorized Reseller), (i) Customer will be the importer of record and responsible for all freight, packing, insurance and other shipping-related expenses; (ii) risk of loss and title to the Tokens will pass to Customer upon delivery of the Tokens by Entrust (or an Authorized Reseller) or one of their respective agents to the carrier; (iii) the Tokens will be free from material defects in materials and workmanship and will conform to the published specifications for such Tokens in effect as of the date of manufacture for a period of one (1) year from the date on which such Tokens are first delivered to Customer (or for such extended warranty period as may be set out in the applicable Order); (iv) Customer will use Entrust as Customer's point of contact for Token warranty inquiries; and (v) as an express condition of the sale, Customer acknowledges that Customer is only permitted to use Tokens with the Hosted Service and Customer is expressly prohibited from using and agrees not to use Tokens with any other provider's verification or identification software even if the Tokens may interoperate with such other provider's verification or identification software. The aforementioned Token warranty will not apply where the issue is caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Token. Any Token that is replaced becomes the property of Entrust. Entrust's exclusive liability and Customer's exclusive remedy for breach of this Section (*Tokens*) is for Entrust, at its option, to repair or replace the Token, or take return of the Token and refund the price paid for the Token.

11.5. Customer Using Hosted Service Provider Functionality for its Affiliates. Where Entrust enables and Customer chooses to utilize the "service provider" functionality in respect of Customer Affiliates, (i) Customer will be permitted to allocate the aggregate number of User entitlements set out on the Order between Customer and its Affiliates, and (ii) each of Customer's Affiliates to which subscriptions are allocated will be deemed to be the Customer for purposes of the Agreement and bound by the terms and conditions of the Agreement as if such Affiliate was Customer itself. Customer agrees to be jointly and severely liable for the performance (or non-performance) of the Agreement by each such Affiliate including, without limitation, any breach of the Agreement, any and all indemnification obligations contained within the Agreement, and any and all acts or omissions of each such Affiliate as if such actions or omission has been performed by Customer

itself. Customer will provide Entrust with prior written notice before adding any Affiliate. Such notice will include each Affiliate's full corporate name and address as well a point of contact within the Affiliate. To the extent Entrust requires additional information about an Affiliate or their usage of the Hosted Service including, without limitation, as part of a lawful access request or subpoena, Customer will make best efforts in co-operating with Entrust. Customer will remain responsible for payment for all fees set out on its Order.

11.6. U.S. Government End-Users. The Software and Documentation are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If the Software and Documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 227.7202-4 (for Department of Defense licenses only) and 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to the Software and Documentation are limited to the commercial rights and restrictions specifically granted in the Agreement. The rights limited by the preceding sentence include, without limitation, any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the Software and Documentation. This Section (*U.S. Government End-Users*) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any legal notice appearing in the Software or Documentation or on any packaging or other media associated with the Software or Documentation.

11.7. Compliance with Applicable Laws. In addition to Customer's compliance obligations in the General Terms, Customer is responsible for ensuring that its use of the Entrust Technology, any Extensions, and any Third Party Integrations, complies with, and Customer will comply with its obligations under all applicable laws, rules or regulations, including, without limitation, all applicable privacy and data protection laws, rules or regulations governing the protection and transfer of Authentication Records, Customer Data and Profiles (including all Personal Data contained therein), and/or Service Data.

11.8. Amendment. This IDaaS Schedule may be amended by Entrust from time to time by posting a new version on its website, and such new version will become effective on the date it is posted except that if Entrust modifies this IDaaS Schedule in a manner which materially reduces Customer's rights or increases Customer's obligations and such changes are not required for Entrust to comply with applicable laws, the changes will become effective sixty (60) days after Entrust provides Customer written notice of changes (email or posting notice at the Hosted Service portal to suffice as adequate notice). If Customer objects in writing during that sixty (60) day period, the changes to this IDaaS Schedule will become effective at the end of Customer's current subscription term. Notwithstanding the foregoing, provisions of this Section (*Amendment*), amendment of the AUP is governed by the AUP. This IDaaS Schedule may not be modified by Customer except by formal agreement in writing executed by both parties.

11.9. Insurance. Customer shall have and maintain in force appropriate insurance with reputable authorized insurers of good financial standing which shall cover the liability of Customer for the performance of its obligations under the Agreement. Customer shall provide to Entrust, upon written request from Entrust but not more than once in any twelve (12) month period, written confirmation from the arranging insurance brokers that such insurances are in effect. The provisions of any insurance or the amount of coverage shall not relieve Customer of any liability under the Agreement. It shall be the responsibility of Customer to determine the amount of insurance coverage that will be adequate to enable Customer to satisfy any liability in relation to the performance of its obligations under the Agreement.

SMS/VOICE VERIFICATION

SPECIAL TERMS AND CONDITIONS

These SMS/Voice Verification Special Terms and Conditions ("Verification Special Terms") are attached to the IDaaS Schedule and contain the terms and conditions that govern access to and use of the SMS + Voice Verification Service (as defined herein). Customer's use of the SMS + Voice Verification Service are subject to these SMS + Verification Special Terms, the IDaaS Schedule terms and conditions, and the General Terms. Capitalized terms not defined in Section 1 herein or elsewhere in these Verification Special Terms shall have the meaning set out in the IDaaS Schedule. References to articles or sections herein shall be to articles or sections in these Verification Special Terms unless otherwise expressly stated. Provisions in these Verification Special Terms will prevail with respect to the SMS + Voice Verification Service over any conflicting provision in the IDaaS Schedule.

1. **DEFINITIONS.**

1.1. "Applicable Law" means any statute, statutory instrument, regulation, order and other legislative provision, including any delegated or subordinate legislation, and any judgment of a relevant court of law or decision of a tribunal or competent authority, to the extent any of the foregoing applies to a party's performance of obligations under the Agreement in the relevant jurisdiction.

1.2. "Customer Data" means any information transmitted by or on behalf of Customer during the execution of an electronic request to the SMS + Voice Verification Service.

1.3. "Inappropriate Content" means any content which (a) is unsolicited, including without limitation, unauthorized "bulk" or "spam" messages; (b) contains or introduces "viruses", "worms", "Trojan Horses", "e-mail bombs", "cancel bots" or other similar computer programming routines; (c) is in any way unlawful; (d) infringes the intellectual property or privacy or other rights of any person, including without limitation the Intellectual Property Rights of Entrust (or its licensors or service providers); or (e) executes, initiates or causes "phishing" or social engineering activities.

1.4. "Intellectual Property Rights" means all trade secrets, patents and patent applications, trademarks, services marks, trade names, internet domain names, copyrights (including copyrights in computer software), moral rights, rights in knowhow and any renewals or extensions of the foregoing, and all other proprietary rights, and all other equivalent or similar rights which may subsist anywhere in the world, including any renewals or extensions thereof.

1.5. "SMS + Voice Verification Service" means the Entrust service which provides real time delivery of a one-time password to a User mobile device by either SMS or a voice channel for verification purposes.

1.6. "User" means any of Customer's customers, clients, or other users that use the SMS + Voice Verification Service in respect of whom Customer Data is submitted.

2. **USE OF SMS AND VOICE VERIFICATION SERVICE**.

2.1. Grant of License. Subject to the terms and conditions of these Verification Special Terms, Entrust hereby grants to Customer a non-exclusive, non-transferable right to use the Service during the term of their eligible active IDaaS subscription or license. Customer may only use the SMS + Voice Verification Service with the IDaaS product which Customer must have acquired from Entrust (or a Reseller). Entrust and/or its licensors retains all right, title, and interest (including all intellectual property rights), in, to and under the SMS + Voice Verification Service.

2.2. Service Interruption. Customer agrees and acknowledges that the SMS + Voice Verification Service may be affected in the following circumstances:

2.2.1. Entrust may temporarily suspend or discontinue the SMS + Voice Verification Service, with advance notice if practicable, at any time if Entrust has reasonable cause to suspect that the SMS + Voice Verification Service is being used to transmit Inappropriate Content or to commit fraud, or if Entrust reasonably believes such action is necessary to avoid an imminent material threat of harm to Entrust, its affiliates, Users or any third party; and

2.2.2. Entrust may, upon two (2) business days' notice, suspend provision of the SMS + Voice Verification Service if (i) any fees are due and unpaid; or (ii) Customer fails to comply with the Use Guidelines set out in Section 2.3 (*Usage Guidelines*) below.

2.3. Use Guidelines. Customer shall:

2.3.1. not use the SMS + Voice Verification Service, in part or in whole, for any purpose or in any way prohibited by any Applicable Laws, or in any manner that may disable, impair, damage or interfere with any Entrust hardware, software, intellectual property rights, the SMS + Voice Verification Service, or any other users of the SMS + Voice Verification Service;

2.3.2. not copy, reverse engineer, modify, create derivative works of, distribute, sell, assign, pledge, sublicense, lease, loan, rent, share, timeshare, grant a security interest, deliver, or otherwise transfer, directly or indirectly, any portion of or rights in the SMS + Voice Verification Service, or any Entrust software (including source code thereto), computer systems or networks, or otherwise make data available (or any portion thereof) to third parties (except to the extent expressly set forth in this Agreement);

2.3.3. not use the SMS + Voice Verification Service, or permit the SMS + Voice Verification Service to be used, to transmit marketing or advertising messages without prior written consent from Entrust, or to transmit Inappropriate Content;

2.3.4. not use the SMS + Voice Verification Service for the purpose of assessing creditworthiness; and

2.3.5. not use the SMS + Voice Verification Service in circumstances in which the failure or delay of the SMS + Voice Verification Service could lead to death, personal injury, physical property damage or environmental damage.

2.4. Intellectual Property Rights. Entrust (or its licensors or service providers) owns all Intellectual Property Rights relating to or embodied in the SMS + Voice Verification Service. The SMS + Voice Verification Service and all modifications, enhancements and derivative works thereof, including all right, title and interest (and all Intellectual Proprietary Rights therein) remain the sole and exclusive property of Entrust and/or its third-party licensors.

2.5. Restrictions. Customer does not acquire any rights, express or implied, in the SMS + Voice Verification Service, other than those rights specified in these Verification Special Terms. Customer shall immediately cease to use the SMS + Voice Verification Service upon (a) expiration of the Subscription Term; (b) reaching any transaction or user limits set out in the Order or Documentation; or (c) upon Customer breach of these Verification Special Terms. Customer hereby consent to the use, transfer, processing and storage of Customer Data as deemed necessary by Entrust, in its sole discretion, in order to provide the SMS + Voice Verification Service to Customer. Customer shall comply with all Applicable Laws including, without limitation, laws relating to Customer use of the SMS + Voice Verification Service, import, export, licensing, privacy protection and data protection laws, as they apply to the activities contemplated under these Verification Special Terms. Customer hereby consents and authorizes Entrust, as may be required by Applicable Laws, to (i) provide the SMS + Voice Verification Service to Customer, and (ii) process Customer Data, including any of Customer personal information.

3. **CUSTOMER DATA & PRIVACY**.

3.1. Data Protection Laws. Customer shall perform its obligations under the Agreement in compliance with all Applicable Laws relating to the protection of privacy and data, in use of the SMS + Voice

Verification Service.

3.2. Customer Data. Entrust (or its licensors and service providers) shall use Customer Data only to provide, maintain, and improve the SMS + Voice Verification Service. Customer Data, including any Personal Data therein, may be stored and processed in the United States or any other countries in which Entrust (or its licensors and service providers) maintains relevant facilities. Customer consents, and shall procure the consent of every Data Subject, to any such transfer and appoints Entrust (or its licensors and service providers) to conduct such a transfer on Customer's behalf in order to provide the SMS + Voice Verification Service.

3.3. Consent. Customer shall provide all Data Subjects with any disclosure or explanation required by Applicable Laws concerning the Customer's use of the SMS + Voice Verification Service, and obtain, maintain and secure any necessary consent and authorizations from Data Subjects that may be required by Applicable Laws in order to authorize Entrust's provision of the SMS + Voice Verification Service, or otherwise ensure a lawful basis for Entrust's provision of the SMS + Voice Verification Service and processing of Customer Data, including any Personal Data.

3.4. Third Party Data Providers. Use of the SMS + Voice Verification Service by Customer may require interaction with third parties such as telecommunications operators. Customer hereby consents to the disclosure by Entrust (or its licensors or service providers) of Customer's (and its Users') identity to such operators, for the limited purpose of such operators ensuring that Entrust (or its licensors or service providers) is complying with the terms of its agreements with such third parties. If any such third party requires Users to provide specific consent to enable the provision of the SMS + Voice Verification Service, Customer shall reasonably cooperate with Entrust (or its licensors or service providers) to confirm the sufficiency of such consent.

3.5. Content of Text Messages (SMS); E-Mails, Etc. All passcodes delivered to Customer or its Users by text messages (SMS), emails or by any other means are, for security reasons, generated randomly and Entrust has no direct influence on the combination of letters and/or numbers generated as passcodes, including any words and meanings of the passcodes. Entrust takes no responsibility for the content or meaning (if any) of the automatically generated passcodes. Customer acknowledges and agrees that, other than the content of the default message templates included in the Software, Entrust: (i) has no direct control over any content, including, without limitation, passcodes, messages (including any modifications to default message templates not made by or on behalf of Entrust), text, script, data, or other information ("Content") delivered to Customer and/or Users, by text messages or by any other means through the Identity Mobile App; and (ii) takes no responsibility to Customer or to any third party for such Content, including any Content which might be false, inaccurate, inappropriate, incomplete, unsuitable, defamatory, libelous, obscene, abusive, intimidating, harmful, fraudulent, a virus or malicious code, spam, or otherwise unlawful or illegal. Customer will indemnify, defend and hold harmless Entrust from and against any third party claims, demands, suits or proceedings, costs, damages, losses, settlement fees, and expenses (including without limitation reasonable attorney fees and disbursements) arising out of or related to any Content.

4. **CUSTOMER WARRANTIES; DISCLAIMER.**

4.1. Customer Warranties, Customer warrants and represents that, in the use of the SMS + Voice Verification Service, it will:

4.1.1. comply with the Use Guidelines;

4.1.2. use of the SMS + Voice Verification Service in compliance with all Applicable Laws; and

4.1.3. obtain and maintain all necessary licenses, consents and permissions necessary for Entrust (and its licensors and service providers) to perform its obligations under the Agreement, including the provision of the SMS + Voice Verification Service.

4.2. Disclaimer. Except as provided for herein, the SMS + Voice Verification Service are subscribed to Customer "AS IS" and with all faults. Except as provided for herein, Entrust (and its licensors and service providers) does not make any representation and/or warranty of any kind whatsoever, either express or implied, in connection with the SMS + Voice Verification Service, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and/or any warranty that provision of the SMS + Voice Verification Service will be uninterrupted or error free. Customer acknowledges that Entrust (and its licensors and service providers) secures information from third party sources and neither Entrust (and its licensors and service providers) nor any of its third party sources warrant that the information will be accurate or error free. Entrust (and its licensors and service providers) further disclaims all warranties not expressly set forth herein, Customer agrees that Entrust (and its licensors and service providers) will not be liable for any content, including but not limited to the content that is sent, received, held, released or otherwise connected in any respect to the SMS + Voice Verification Service, content that is sent but not received, and content sent using and/or included in the SMS + Voice Verification Service (including without limitation any threatening, defamatory, obscene, offensive, or illegal content), or any access to or alteration of content.

5. **INDEMNITIES.**

5.1. In addition to Customer's indemnification obligations pursuant to Section 8.1 (*Indemnification by Customer*) of the IDaaS Schedule, Customer further agrees to defend, indemnify and hold harmless, Entrust against any and all third party claims, demands, suits or proceedings, costs, damages, losses, settlement fees, and expenses (including without limitation attorney fees and disbursements) arising out of or related to: (i) any willful or intentional misconduct by Customer; (ii) any breach by Customer of its warranties in Section 4.1.1; or (iii) any breach by Customer of its warranties in Sections 4.1.2 and 4.1.3. "Customer-Related Claims" shall include, for the purposes of these Verification Special Terms, the foregoing additional indemnification obligations.

6. **TERMINATION.**

6.1. Entrust Termination or Suspension for Cause. Entrust may, at its sole discretion, suspend or terminate Customer's and/or Users' access to SMS + Voice Verification Service at any time, without advanced notice, if: (i) Entrust reasonably concludes that Customer and/or its Data Subjects have conducted themselves in a way (a) that is not consistent with or violates the requirements of the Documentation, the Usage Guidelines, or is otherwise in breach of the Agreement; (b) in a way that subjects Entrust to potential liability or interferes with the use of SMS + Voice Verification Service by other Entrust customers and/or users; or (c) in Entrust's reasonable opinion, be likely to result in material harm to Entrust (or its licensors and service providers), the SMS + Voice Verification Service, or Entrust's (or its licensors' and service providers') other customers; (ii) Entrust has reasonable cause to suspect that the SMS + Voice Verification Service is being used to transmit Inappropriate Content or to commit fraud, or if Entrust reasonably believes such action is necessary to avoid an imminent material threat or harm to Entrust, its Affiliates, licensors, service providers, or channel partners, or any other third party; (iii) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' and/or users' information or data processed by SMS + Voice Verification Service; or (iv) Entrust reasonably concludes that Customer and/or Users are violating Applicable Laws. Entrust may also, without notice, suspend Customer's and/or its Data Subjects' access to SMS + Voice Verification Service for scheduled or emergency maintenance. Termination of these Verification Special Terms will not necessarily result in termination of the entire Agreement (e.g. if Customer has an Identity Enterprise license and the applicable Order may still be active).

6.2. Entrust Termination for Convenience. Entrust may terminate Customer's entitlement to the SMS + Voice Verification Service for any or no cause with ninety (90) days prior written notice.

GEOIP DATABASE

SPECIAL TERMS AND CONDITIONS

These GeoIP Database Special Terms and Conditions ("GeoIP Database Special Terms") are attached to the IDaaS Schedule, and contain the terms and conditions that govern access to and use of the Databases (as defined herein). Customer's use of the Databases is subject to these GeoIP Database Special Terms, the IDaaS Schedule terms and conditions, and the General Terms. Capitalized terms not defined in Section 1 herein or elsewhere in these GeoIP Database Special Terms shall have the meaning set out in the IDaaS Schedule. References to articles or sections herein shall be to articles or sections in these GeoIP Database Special Terms unless otherwise expressly stated. Provisions in these GeoIP Database Special Terms will prevail with respect to the Databases over any conflicting provision in the IDaaS Schedule.

1. **DEFINITIONS.**

1.1. "Applicable Law" means any statute, statutory instrument, regulation, order and other legislative provision, including any delegated or subordinate legislation, and any judgment of a relevant court of law or decision of a tribunal or competent authority, to the extent any of the foregoing applies to a party's performance of obligations under the Agreement in the relevant jurisdiction.

1.2. "GeoIP Data" means data available through the GeoIP Databases.

1.3. "GeoIP Database(s)" means database services and products which include updated Internet protocol ("IP") address data and fields (including without limitation Internet Servicer Provider, organization name, and autonomous system organization and number associated with an IP address, country, subdivisions, city, postal code, latitude, and longitude and other geographic information and other data associated with an IP address), patches, bug fixes, and similar corrections ("Updates") that provide the geographic information and other data associated with specific IP addresses.

2. **USE OF DATABASES**.

2.1. Grant of License. Subject to the terms and conditions of these GeoIP Database Special Terms, Entrust hereby grants to Customer a non-exclusive, non-transferable right to use the GeoIP Databases during the term of their eligible active IDaaS subscription or license. Customer may only use the GeoIP Databases with the IDaaS product which Customer must have acquired from Entrust (or a Reseller). Entrust and/or its licensors retains all right, title, and interest (including all intellectual property rights), in, to and under the GeoIP Databases; no title to such intellectual property rights is transferred to Customer. Any copies of the GeoIP Databases made by Customer (i) will be used only for purposes consistent with the rights expressly granted in this Agreement; and (ii) will contain all of the original Entrust (or Entrust licensor) notices regarding proprietary rights.

2.2. GeoIP Data Included. For the purposes of these GeoIP Database Special Terms, GeoIP Databases are inclusive of the GeoIP Data, and all references to the GeoIP Databases shall be deemed to include the GeoIP Data contained therein.

2.3. Trade Secrets. Customer acknowledges and agrees that the GeoIP Databases constitute the proprietary trade secrets of Entrust (and its licensors).

2.4. Restrictions. Except as expressly permitted by these GeoIP Database Special Terms, Customer agrees not to (or allow any third parties to):

2.4.1.use, copy or distribute any portion of the GeoIP Databases;

2.4.2.use the GeoIP Databases to develop a database, info base, online or similar database

service, or other information resource in any media (print, electronic or otherwise, now existing or developed in the future) for sale to or use by others;

2.4.3. reproduce or distribute the GeoIP Databases in a manner which allows its customers or users to access the GeoIP Databases in a way other than through IDaaS;

2.4.4. use the GeoIP Data to create or otherwise support the transmission of unsolicited, commercial email;

2.4.5. remove, disable, or defeat any functionality in the GeoIP Databases designed to limit or control access to or use of the GeoIP Databases;

2.4.6. reverse assemble, reverse engineer, decompile, reverse decompile, reduce to human perceivable form, or otherwise attempt to derive source code from the GeoIP Databases;

2.4.7. modify, incorporate into or with other software, or to create derivative works of, the GeoIP Databases;

2.4.8. remove, alter or obscure any copyright or other proprietary notices incorporated on or in the GeoIP Databases by Entrust (or its licensors);

2.4.9. make the GeoIP Databases available to third parties, including through file sharing, or to transfer or sublicense the GeoIP Databases or allow the GeoIP Databases to become subject to any lien; and

2.4.10. use the GeoIP Databases for the purpose of identifying or locating s specific individual or household.

3. **CUSTOMER DATA & PRIVACY**.

3.1. Data Protection Laws. Customer shall perform its obligations under these GeoIP Database Special Terms in compliance with all Applicable Laws relating to the protection of privacy and data, in use of the GeoIP Databases.

3.2. Customer Data. Entrust (or its licensors and service providers) shall use Customer Data only to provide, maintain, and improve the GeoIP Databases. Customer Data, including any Personal Data therein, may be stored and processed in the United States or any other countries in which Entrust (or its licensors and service providers) maintains relevant facilities. Customer consents, and shall procure the consent of every Data Subject, to any such transfer and appoints Entrust (or its licensors and service providers) to conduct such a transfer on Customer's behalf in order to provide the GeoIP Databases.

3.3. Consent. Customer shall provide all Data Subjects with any disclosure or explanation required by Applicable Laws concerning the Customer's use of the GeoIP Databases, and obtain, maintain and secure any necessary consent and authorizations from Data Subjects that may be required by Applicable Laws in order to authorize Entrust's provision of the GeoIP Databases, or otherwise ensure a lawful basis for Entrust's provision of the GeoIP Databases and processing of Customer Data, including any Personal Data.

3.4. Destruction of Old Versions. From time to time, Entrust (or its licensors) may release updated versions of the GeoIP Databases. Customer agrees to promptly use the updated version of the GeoIP Databases and cease use of any old versions. Customer shall promptly delete (i) all old versions of the GeoIP Databases upon release of the updated versions; and (ii) all GeoIP Databases upon termination of their IDaaS subscription.

4. **WARRANTY DISCLAIMER.**

4.1. Disclaimer. The disclaimer of warranties in the General Terms shall apply to the GeoIP Databases.