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"), 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 Entrust's acceptable use policy, as may be modified from time to time, available on Entrust's website at https://www.entrust.com/-/media/documentation/productsupport/entrust-idaas-aup.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 (or its sub-processors) 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 platform which Entrust hosts on its (or its hosting providers') computers.

1.10. "Professional Services" means professional services made available in relation to the Entrust Technology as described in Documentation, and that incorporate by reference the Professional Services Special Terms and Conditions. Professional Services shall not include Support Services.

1.11. "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.

1.12. "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.

1.13. "SLA" means Entrust's standard service level agreement for the Hosted Service, as may be modified from time to time, available on Entrust's website at https://www.entrust.com/-/media/documentation/productsupport/entrust-idaas-sla.pdf.

1.14. "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.

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

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

1.17. "Third-Party Integrations" has the meaning set out in Section 5.9 (*Third-Party Integrations*).

1.18. "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.; (v) for the sole purpose of authenticating the identity of Users; and (vi) subject to the general restrictions set out in Section 8 of the General Terms (*General Restrictions*).

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. Customer receives no rights to the Software other than those specifically granted in Section 2.2 (Software).

2.2.1. License. Subject to Customer's compliance with the Agreement, Entrust hereby grants Customer a personal, non-exclusive, non-transferable, non-sub-licensable license to download, install, and use the Software, in object code form only, for the sole purpose of conducting Customer's internal business operations, and not for resale or any other commercial purpose, all in accordance with: (i) the Documentation; and (ii) any specifications or limitations set out in the Order or imposed by technological means of the capabilities of the Software that Customer is permitted to use.

2.2.2. Licensed Not Sold. Copies of the Software provided to Customer pursuant to the Agreement are licensed, not sold, and Customer receives no title to or ownership of any copy of the Software itself. Furthermore, Customer receives no rights to the Software other than those specifically granted in Section 2.2.1 (*License*) above.

2.2.3. Hosting and Management. Customer agrees that it will be responsible for installing and managing the Software on its own premises in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Hosted Service resulting from Customer's improper installation and/or management of the Software.

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 [insert appropriate link] 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. 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. Service Regions. Customer will select the geographic region(s) (each a "Service Region") where Authentication Records, Customer Data, Profiles and Service Data will be stored (subject to any limitations of Entrust's hosting providers). With respect to the Authentication Records, Customer Data, Profiles and Service Data, and any Personal Data contained therein, that Entrust may collect hereunder, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Notwithstanding the foregoing, Customer acknowledges and agrees: (i) that Entrust may send short message service (SMS) messages through the United States and/or Canada as part of the Entrust Technology; and (ii) Customer's billing information may be stored in the United States and/or Canada.

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.

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 10 (*Liability*), 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 part 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. 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) a violation of applicable law by Customer or its Users, or in relation to Customer Data; (iv) 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; (v) a dispute between Customer and any User, or a claim by a User; (vi) 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 (vii) Customer use of the Entrust Technology in breach of 3.1 (*Evaluation Purposes*), or 3.2 (*Not-For-Resale* (*NFR) Purposes*) (each of (i)-(vii), 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. Miscellaneous.

10.1. 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.

10.2. 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.

10.3. 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).

10.4. 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.

10.5. 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.

10.6. 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.

10.7. 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.

10.8. 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.

10.9. 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.

Identity Proofing Special Terms and Conditions

These Identity Proofing Special Terms and Conditions ("ID Proofing Special Terms") are attached to the IDaaS Schedule, and contain the terms and conditions that govern access to and use of Identity Proofing (as defined herein). Capitalized terms not defined in Section 1 herein or elsewhere in these ID Proofing 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 ID Proofing Special Terms unless otherwise expressly stated. Provisions in these ID Proofing Special Terms will prevail with respect to Identity Proofing over any conflicting provision in the IDaaS Schedule.

1. **DEFINITIONS.**

1.1. "Customer Application" means the application developed by Customer pursuant to the SDK License (as defined herein) to be used to access and use Identity Proofing.

1.2. "Customer Data", in addition to its meaning in the IDaaS Schedule, with respect to Identity Proofing means Device Information, Risk Information, Identity Proofing Results, as well as data or information collected using the Customer Application.

1.3. "Database" means the centralized Global Intelligence Platform owned, operated and maintained by Entrust (or its service providers) which contains Device Information and associated information including Risk information.

1.4. "Device" means a particular computer, mobile phone, desktop, tablet or other computing device.

1.5. "Device Information" means a set of Device attributes and characteristics that are designed to identify a particular Device.

1.6. "Identity Proofing" means the identity proofing functionality which forms part of the Hosted Service (if such functionality is selected by Customer and approved by Entrust in an Order).

1.7. "Identity Proofing SLA" means the Entrust's service level agreement specific to Identity Proofing, as set out in Attachment A to these ID Proofing Special Terms.

1.8. "Response" means the recommendation, including Risk Information, returned by Identity Proofing about a Device which has been evaluated by Identity Proofing.

1.9. "Risk" means risk including, without limitation, transaction, abuse, reputation and fraud risk.

1.10. "Risk Information" means information relating to specific Risk(s).

1.11. "SDK License" means the Entrust Mobile ID Proofing SDK License through which Customer may obtain a license to use the Mobile ID Proofing software development toolkit. The SDK License is not a part of the Agreement.

1.12. "User" has the meaning set out in the General Terms, and in these ID Proofing Special Terms includes any individual end user who accesses and/or uses Identity Proofing through the Customer Account, via the Customer Application.

2. **USE OF IDENTITY PROOFING.**

2.1. Grant of License. Subject to Customer's compliance with the Agreement, Entrust grants to Customer, during the ID Proofing Term (as defined herein), a worldwide, non-exclusive, nontransferable, non-sub-licensable right to, all in accordance with the Documentation, provide its User(s) with access to and/or use of Identity Proofing, through the Customer Account, via the Customer Application:

2.1.1. for the purpose of authenticating the identity of a User, extracting identity information or data from the User's identity document(s), and sending authentication results (resulting from (i) through (iv) above) to Customer ("Identity Proofing Results"), and not for resale or any other commercial purpose;

2.1.2. for the purpose of collecting and processing Device Information and providing Responses to Customer.

2.2. Restrictions. Identity Proofing shall not be available: (i) to MSPs or Tenants (as such terms are defined in the Managed Security Service Provider Special Terms and Conditions); and/or (ii) for not-for-resale (NFR) purposes.

2.3. Service Levels. The sole remedies for any failure of Identity Proofing are listed in the Identity Proofing SLA. Service credits issued pursuant to the Identity Proofing 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.

3. **CUSTOMER DATA & PRIVACY.**

3.1. Service Regions. The Service Regions available for selection by Customer may be different for Identity Proofing than for the main components of the Hosted Service, depending on the nature of the Customer Data, Personal Data, or Service Data (and the related Entrust hosting provider). With respect to the Customer Data and Personal Data that Entrust may collect pursuant to Identity Proofing, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Customer further grants to Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers), a world-wide, limited right, during the ID Proofing Term, to host, copy, transmit and display 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 Identity Proofing in accordance with the Agreement.

3.2. Excluded Data (Exception). Notwithstanding the provisions set out in Section 12.2 of the General Terms, Identity Proofing may involve the processing of Excluded Data. As such, Section 12.2 of the General Terms shall not apply with respect to any Excluded Data that is necessary or required in order for Entrust to provide Identity Proofing to Customer and its Users pursuant to the Agreement, but only to the extent necessary or required. Customer acknowledges and agrees that the provisions of Section 12.2 of the General Terms shall continue to apply in all other cases, along with all other disclaimers, limitations and exclusions contained in the IDaaS Schedule.

3.3. Consents; Accuracy; Rights. Customer represents and warrants that, before authorizing a User to use Identity Proofing and before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite rights, consents or permissions, 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 contained therein, by Entrust

(including any of its Affiliates, and any of their respective applicable subcontractors and hosting providers) in accordance with the Agreement. Customer further represents and warrants to Entrust that such Customer Data or Personal Data is accurate and up-to-date (and that Customer shall correct or update it as required), and that no Customer Data or Personal Data will violate or infringe (i) any third-party intellectual property, publicity, privacy or other rights; (ii) any applicable laws, rules or regulations or the AUP; or (iii) any third-party products or services terms and conditions. Customer will be fully responsible for any Customer Data or Personal Data submitted, uploaded, or otherwise provided to Identity Proofing by any User as if it was submitted, uploaded, or otherwise provided by Customer. Customer is solely responsible for the accuracy, content and legality of all Customer Data and Personal Data.

3.4. Rights in Customer Data and Personal Data. As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data and Personal Data provided to Entrust. Subject to the terms of the Agreement, Customer hereby grants to Entrust a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data and Personal Data contained therein solely to the extent necessary to provide Identity Proofing to Customer, and to sub-license such rights to any of Entrust's applicable subcontractors.

3.5. Rights in Certain Data (Device Reputation). As between the parties, Entrust owns and will retain all right, title and interest (including but not limited to any copyright, patent, trade secret, trademark or other proprietary and/or intellectual property rights) in and to Identity Proofing, and the Device Information, Database, and any Response. For clarity, the foregoing does not mean that Entrust owns or retains any right, title or interest in or to the data elements comprising the Device Information, the Database, or any Response. The foregoing is an acknowledgement that, as between the parties, Entrust will retain any right, title and interest it may have in the Device Information, Database, and any Response, as collective works. Customer acknowledges that the Device Information and the Database, as collective works, may be Confidential Information of Entrust.

4. CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS.

4.1. Compliance with Laws. Customer represents, warrants and covenants that is shall (i) use commercially reasonable efforts to prevent unauthorized access to, or use of, Identity Proofing and shall notify Entrust as soon as possible if it becomes aware of any unauthorized access or use of Identity Proofing; (ii) use Identity Proofing only for lawful purposes; (iii) not knowingly violate any law, rules or regulations of any country with its use of Identity Proofing; and (iv) not knowingly violate the intellectual property rights of any third party with its use of Identity Proofing.

4.2. Users; Identity Proofing Access. . Customer is responsible and liable for: (a) handling, use, and/or consequences or impact of Results or Responses resulting from use of Identity Proofing (e.g. impact on User's credit rating or ability to open accounts or any other unfavorable impact).

5. TERM, TERMINATION & SUSPENSION.

5.1. Term. Unless otherwise specified in the Order that includes the subscription for Identity Proofing, these ID Proofing Special Terms will commence on the date the Order is accepted by Entrust, and will remain effective for the subscription period specified for Identity Proofing in the Order, unless terminated earlier in accordance with the Agreement ("ID Proofing Term"). Upon expiration of the ID Proofing Term, Customer may elect to renew its subscription pursuant to these ID Proofing Special Terms for an additional length of time, as set forth in an Order for renewal, in which case the ID Proofing Term for Identity Proofing will be extended to include such additional length of time upon

payment of the applicable fees for the additional length of time, all as set out in the Order for renewal.

5.2. Termination or Suspension for Cause. Entrust may, at its sole discretion, suspend or terminate Customer's and/or Users' access to Identity Proofing at any time, without advanced notice, if: (a) Entrust reasonably concludes that Customer and/or Users have conducted themselves in a way (i) that is not consistent with or violates the requirements of the AUP, the Documentation, or is otherwise in breach of the Agreement; or (ii) in a way that subjects Entrust to potential liability or interferes with the use of Identity Proofing by other Entrust customers and/or users; (b) 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 Identity Proofing; or (c) Entrust reasonably concludes that Customer and/or Users are violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's and/or User's access to Identity Proofing for scheduled or emergency maintenance. Termination of these ID Proofing Special Terms will not necessarily result in termination of the entire Agreement (e.g. if Customer has an Identity as a Service subscription then the IDaaS Schedule and the applicable Order may still be active).

5.3. Effects of Termination. Upon termination or expiration of these ID Proofing Special Terms, Entrust will have no further obligation to provide Identity Proofing to Customer, Customer will immediately cease all use of Identity Proofing, and Customer will return all copies of Confidential Information to Entrust or certify, in writing, the destruction thereof, destroy any copies of Customer Data, Personal Data, Service Data, and Documentation (unless continued rights to use exist pursuant to the Agreement (e.g. if Customer continues to have an Identity as a Service subscription despite the termination or expiry to these ID Proofing Special Terms). 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.

Attachment A

To Identity Proofing Special Terms and Conditions

Identity Proofing SLA

Service Commitment
Entrust will use commercially reasonable efforts to make Identity Proofing available 99.8% of the time during any monthly billing cycle. In the event Identity Proofing does not meet the 99.8% target, Customer will be eligible to receive a Service Credit as described below.

Definitions. Capitalized terms not defined in this Attachment A shall have the meaning set out in the ID Proofing Special Terms.

- "**Monthly Uptime Percentage**" is calculated by subtracting from 100% the percentage of minutes during the month in which Identity Proofing was unavailable. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Exclusion (as defined below).

- "**Service Credit**" is, for the purposes of this Attachment A, a dollar credit, calculated as set forth below, that will be credited by Entrust to Customer's future invoices.

Service Credits
Service Credits are calculated based on the number of transactions that could have been processed during the downtime x the transaction fee that would have been paid by Customer if those transactions had been processed.

If the downtime is less than a full hour:
Step 1 – Calculate the Number of Transactions Processed During the Previous Calendar Quarter. The number of transactions that could have been processed is calculated based on the total number of transactions actually processed by Entrust on Customer's behalf during the calendar quarter immediately preceding the date on which the downtime occurred.

Step 2 – Calculate the Total Number of Hours in the Calendar Quarter. Calculate the number of days in the calendar quarter and multiply by 24 hours per day.

Step 3 – Divide Step 1 by Step 2 to arrive at the average number of transactions processed per hour during the previous calendar quarter:

$$\frac{\text{Step 1}}{\text{Step 2}} = \text{Average Number of Transactions Processed Per Hour}$$

Step 4 – Divide the amount of actual downtime by 60 minutes to arrive at the pro rata amount of an hour that the downtime represents:

$$\frac{\text{Minutes of Downtime}}{60} = \text{Pro Rata Portion of 1 Hour Represented by the Downtime}$$

Step 5 – Multiply the result of Step 4 (the pro rata portion of 1 hour represented by the downtime) by the result of Step 3 (the average number of transactions processed per hour) to arrive at the number of transactions that could have been processed during the downtime:

Step 4 x Step 3 = the Number of Transactions that Could Have Been Processed During the Downtime

Step 6 – Multiply Step 5 by the appropriate fee set forth in the applicable Order.

Step 5 x Transaction Fee = Service Credit

A Service Credit will be issued for the amount arrived at in Step 6.

If the downtime is a full hour:
For any full hour of unavailability, the Customer will receive a Service Credit for the number of transactions that could have been processed in the hour (Step 3) multiplied by the Transaction Fee set forth in the applicable Order.

Example:

- **Step 1** = 5,000 transactions during the previous calendar quarter
- **Step 2** = 91 days in the calendar quarter x 24 hour/day = 2,184 hours during the quarter
- **Step 3** = 5,000 (Step 1) divided by 2,184 (Step 2) = 2.5 transactions processed per hour
- **Step 4** = Assume downtime = 65 minutes so 60 minutes is one full hour leaving 5 minutes for the balance of the calculation. Divide 5 minutes by 60 minutes = 8.3% of an hour is represented by the downtime
- **Step 5** = 8.3% (Step 4) x 2.5 transactions processed during an hour (Step 3) = 1 transaction when rounded up to a whole transaction
- **Step 6** = 1 (Step 5) x $1.00 (transaction fee per transaction) = Service Credit of $1.00
- **Step 7** = Service Credit for less than a full hour (Step 6) + average number of transactions processed per hour (Step 3) multiplied by the transaction fee per transaction or $1 transaction fee + (2.5 average hourly transactions x $1 transaction fee) = $3.5 Service Credit for 65 minutes of downtime

Credit Request and Payment Procedures
Within thirty (30) days of the end of the relevant calendar month, Customer must submit a written request to Entrust for a Service Credit, along with sufficient information for Entrust to verify the time(s) and date(s) of the event for which Customer is claiming a Service Credit. If the Monthly Uptime Percentage when calculated by Entrust falls below the Uptime Guarantee, then Entrust will notify Customer that a Service Credit will be issued to Customer within one billing cycle following the month in which such request was confirmed by Entrust and the amount of the Service Credit. Customer's failure to request a Service Credit in a timely manner or provide sufficient information to Entrust that Entrust may reasonably request in order to verify the Monthly Uptime Percentage will disqualify Customer from receiving a Service Credit.

Exclusions

Exclusions shall not be included in the calculation of the time Identity Proofing was available in any given calendar month. As used herein, "Exclusion" shall mean any unavailability: (i) due to Entrust's planned maintenance or downtime the occurrence of which Customer received at least 24-hour advance written notice; (ii) caused by factors outside of Entrust's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Identity Proofing; (iii) that result from the Customer Application, or failure of equipment, software, technology or facilities provided by Customer, including but not limited to, network unavailability or bandwidth limitations outside of Entrust's network; (iv) that results from a failure of the device reputation functionality made available as part of Identity Proofing; or (v) arising from Entrust's suspension and termination of Customer's right to use Identity Proofing in accordance with the Agreement.

Professional Services Special Terms and Conditions

These Professional Services Special Terms and Conditions ("PS Special Terms") are attached to the Entrust Identity as a Service IDaaS Schedule ("IDaaS Schedule") and contain the terms and conditions applicable for Professional Services. Capitalized terms not defined in Section 1 herein or elsewhere in these PS 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 PS Special Terms unless otherwise expressly stated. Provisions in these PS Special Terms will prevail with respect to Professional Services over any conflicting provision in the IDaaS Schedule.

1. **DEFINITIONS.**

1.1. "Background IPR" means any intellectual property rights of a party or its Affiliates conceived, created, developed, or reduced to practice prior to, or independently of, the Professional Services provided under these PS Special Terms.

1.2. "Foreground IPR" means any intellectual property rights conceived, created, developed or reduced to practice by Entrust in the course of providing the Professional Services under these PS Special Terms.

2. **PROFESSIONAL SERVICES.**

2.1. Subject to Customer's compliance with the Agreement, Entrust shall perform the Professional Services for Customer as further described in an Order and any related Documentation.

2.2. Customer shall make available to Entrust any equipment, material, information, data and remote access as Entrust may reasonably require to perform the Professional Services.

2.3. Customer shall also provide Entrust with timely access to appropriate members of the Customer's staff as may be reasonably required by Entrust for the provision of the Professional Services (e.g. answering technical questions, other general questions as they may arise, and availability for meetings). Customer shall be responsible for the timely performance of its obligations under these PS Special Terms with respect to the requirements of Entrust in accordance with these PS Special Terms. Customer acknowledges that any delay on its part in the performance of its obligations may affect or delay Entrust's provision of the Professional Services.

2.4. Professional Services will be delivered remotely during Entrust regular business hours. No visits to Customer premises are included within the Professional Services, and no travel is required by or included within the Professional Services. Customer must provide Entrust remote access to systems as required for delivery of the Professional Services.

2.5. Each party shall designate a primary point of contact for matters relating to the Professional Services.

2.6. Out-of-Scope. Professional Services shall not include the following, which shall be Customer's responsibility: (i) initial setup (licensing, installation/deployment, configuration, verification) of the underlying non-Entrust infrastructure, including, without limitation, hardware, soft tokens, hard tokens, operating system (OS), software, client or virtual machines (VM); (ii) network, database, repository connectivity; (iii) configuration of network, firewall, load balancer, server or repository; (iv)

configuration of third-party applications which will integrate with Entrust applications, other than where explicitly stated within the definition of the Professional Services; (v) any required Entrust software, seed files, and licenses

2.7. Warranty. Entrust represents to the Customer that the Professional Services performed pursuant to these PS Special Terms shall be performed in a professional manner in keeping with reasonable industry practices.

2.8. Non-Solicitation. Customer agrees that, without the prior written approval of Entrust, neither it nor its Affiliates will offer employment to any employees of Entrust nor will it directly or indirectly induce such employees to terminate their employment with their employer. This section is enforceable throughout the term of these PS Special Terms and shall survive for one (1) year following its termination for any reason.

3. **INTELLECTUAL PROPERTY**.

3.1. The Professional Services provided by Entrust pursuant to this Agreement are not "works for hire".

3.2. The Background IPR of a party or its Affiliate shall remain the exclusive property of such party or its Affiliate and shall be deemed to be the Confidential Information of such party.

3.3. All right, title and interest in, to and under the Foreground IPR embodied in the Professional Services shall vest in and be owned by Entrust and shall be deemed to be the Confidential Information of Entrust.

3.4. In respect to the Foreground IPR and any Background IPR of Entrust (and its Affiliates) incorporated in a deliverable provided during the performance of the Professional Services, the Customer and its Affiliates are hereby granted a non-exclusive, non-transferable, royalty-free, worldwide, perpetual license to make, have made, use, copy and disclose such Foreground IPR and Background IPR, but solely to the extent necessary to use and exploit the deliverables provided during the performance of the Professional Services and only so long as such Foreground IPR and Background IPR is embedded in the deliverables and not separated therefrom. Any third party which receives such Foreground IPR and Background IPR shall be advised by the Customer in writing at the time of or before such disclosure, that proprietary confidential information is being communicated and that such information is to be kept confidential and not used except as permitted, and provided further, such third party undertake, in writing, prior to any such disclosure, to respect such obligations of confidence.

3.5. In respect to any Background IPR of the Customer and its Affiliates disclosed to Entrust and/or its Affiliates, Entrust and its Affiliates are hereby granted a non-exclusive, non-transferable, royalty-free, worldwide license for the term of this Agreement to make, use and copy such Background IPR, but solely to the extent necessary to provide the Professional Services to the Customer pursuant to these PS Special Terms.

3.6. Except as explicitly provided herein, no other license is granted under any intellectual property rights.

3.7. Nothing in these PS Special Terms shall prevent Entrust or its Affiliates from providing to a third party the same or similar professional services as those provided to the Customer pursuant to these PS Special Terms. The foregoing is subject to Entrust not breaching any of Customer's proprietary rights.