Identity Enterprise

End User License Terms and Conditions

The Agreement for Entrust's Identity Enterprise Offering ("Identity Enterprise") is made up of these end user license terms and conditions (the "IDE Schedule"), the Entrust General Terms and Conditions available at ("General Terms"), and an Order for Identity Enterprise. 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.**

1.1. "CAL" or "Client Access License" means a license enabling or permitting the use of certain capabilities in respect to a specific individual end user or a specific Device, on a single (1) instance of the Software.

1.2. "Customer Data" means any content, data, or information (including, third-party content, data, or information) that is supplied to Entrust (or its licensors or service providers) in connection with Customer's use of the Entrust Technology. Customer Data may include Personal Data.

1.3. "Data Subject" has the meaning set out in the DPA.

1.4. "Device" means a computer, desktop, workstation, tablet, terminal, telephone, mobile phone, server or other electronic or computing device.

1.5. "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, 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.

1.6. "Entrust Technology" means the Software and any related Documentation.

1.7. "Hardware" shall have the meaning set out in Section 2.9.1 (*Hardware (Default Provisions)*).

1.8. "Licensing String" means a data key provided by Entrust for the purpose of setting the number of CALs or otherwise enabling or controlling certain capabilities within the Software.

1.9. "Special Terms and Conditions" mean any terms and conditions attached to this IDE Schedule.

2. **Software Licenses.**

2.1. Grant of 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, such as limits associated with subscription or transaction levels, as well as on copies of Software, numbers or types of users or devices, number of CALs, and types of deployment (e.g. high availability, test or disaster recovery).

2.2. Licensed Not Sold. The Software is protected by copyright and other intellectual property laws and treaties. Copies of the Software provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software itself.

2.3. Upgrades. This Software Schedule does not grant any entitlement to receive any upgrades to the Software. If Customer is entitled to receive upgrades to any Software, for example as a result of purchasing maintenance and support under a separate Support Schedule or subscribing to an Offering that includes Support with upgrades for the connected Software, then such Software includes such upgrades, subject to any additional terms that may be imposed on enhanced features made available as part of the upgrade.

2.4. Restrictions. In addition to the restrictions set out in the General Terms, Customer shall not: (i) use the Software for service bureau or time-sharing purposes; (ii) permit any unauthorized third parties from accessing the Entrust Technology; or (iii) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Software or the data contained therein.

2.5. License Strings. If an item of Software uses a Licensing String, Customer shall only use such Licensing String in conjunction with the copy of Software for which it was delivered, and Customer may not copy or alter a Licensing String or use it for more than one (1) instance of the Software. All quantities are total quantities. For example, if Customer acquires a license for five (5) copies of an item of Software and acquires 10,000 CALs for such Software, then a total of 10,000 CALs can be used with the Software (i.e. Customer have not purchased 50,000 CALs).

2.6. Installation and Management. Customer agrees that it will be responsible for installing, configuring, and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software resulting from Customer's improper installation, configuration, and/or management.

2.7. Documentation. Customer may reproduce and use the Documentation solely as necessary to support Customer's access to and use of the Software. 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.

2.8. Support. If an Order calls for support, any such support will be provided pursuant to the terms and conditions set out at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf. Notwithstanding the foregoing, where support is purchased through an authorized reseller and the Order indicates that the authorized reseller will provide support, then such support will be provided by the authorized reseller (and not Entrust). If Customer is entitled to receive upgrades to any Software as a result of purchasing maintenance and support, then such Software includes such upgrades, subject to any additional terms that may be imposed on enhanced features made available as part of the upgrade.

2.9. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Entrust Technology, including, without limitation, by protecting its passwords and other log-in information. 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.

2.10. Hardware.

2.10.1. Hardware (Default Provisions). If an Order calls for hardware and no third party or Entrust separate agreements or terms and conditions accompany them, then the Agreement shall apply to such hardware ("Hardware") along with the following terms and conditions: (i) Customer will be the importer of record for the Hardware and responsible for all freight, packing, insurance and other shipping-related expenses; (ii) risk of loss and title to the Hardware will pass to Customer upon delivery of the Hardware by Entrust or one of their respective agents to the carrier; (iii) the Hardware will be free from material defects in materials and workmanship and will conform to the published specifications for such Hardware in effect as of the date of manufacture for a period of one (1) year from the date on which such Hardware are first delivered to Customer (or for such extended warranty period as may be set out in the applicable Order); and (iv) Customer will use Entrust as Customer's point of contact for Hardware warranty inquiries. The aforementioned Hardware warranty will not apply where the issue is caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Hardware. Any Hardware that is replaced becomes the property of Entrust. Entrust's exclusive liability and Customer's exclusive remedy for breach of this Section (*Hardware (Default Provisions)*) is for Entrust, at its option, to repair or replace the Hardware, or take return of the Hardware and refund the price paid for the Hardware. "Hardware" is not part of the Entrust Technology.

2.10.2. Use Only with Software. Any Hardware included with the Software may be used only with the applicable Software, unless otherwise permitted in the applicable agreement accompanying such Hardware, or as otherwise permitted by Entrust in writing.

2.11. Delivery. Entrust shall make the Entrust Technology available for electronic download within thirty (30) days of acceptance of an Order, subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for and bear all expenses (including taxes) related to making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

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 shall 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 that is an authorized reseller of the Entrust Technology the right to download, install, access, and use the Entrust Technology for not-for-resale (NFR) purposes for the NFR Period. During the NFR Period Customer 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 - only fictitious non-production data can be used.

3.3. Trial Period. Customer's evaluation of the Entrust Technology pursuant to this Section 3 (*Evaluation; NFR*) shall commence on the date Customer downloads and/or accesses the Entrust Technology and continue for a period of thirty (30) days ("Trial Period"), or as otherwise agreed to

by Entrust in writing with Customer (authorized reseller).

3.4. 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 the date Customer downloads and/or accesses the Entrust Technology and continue for the duration indicated in the Order or the Documentation ("NFR Period").

3.5. Termination. Notwithstanding the foregoing, Entrust may in its sole discretion 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.**

4.1. Customer will pay the costs and fees (including where overages are applicable, any overage fees) for the Software (or Hardware, if applicable) as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

5. **Data Processing.**

5.1. Consents Customer Data; Personal Data. Customer represents and warrants that before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite consents (if any) and made all requisite disclosures (if any) to data subjects, in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data, by Entrust (or its licensors or service providers) in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Customer Data or Personal Data and the means by which Customer acquired them.

6. **No Other Rights Granted; Feedback.**

6.1. No Other Rights Granted. The rights granted under the Agreement are only as expressly set forth in the Agreement. No other right or interest is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of the Agreement or any conduct of either party under the Agreement. Entrust and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by Entrust (including any modifications, enhancements and derivative works thereof). Any permitted copy of all or part of any item provided to Customer must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust to Customer.

6.2. 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; Disclaimer.**

7.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery the Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

7.2. Warranty Exclusions. The warranty in Section 7.1 (*Software Warranty*) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Software; (iii) any modifications or additions made to the Software by Customer. Entrust shall have no obligation to fix errors in the Software caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Software; or (iv) any evaluation or NFR use pursuant to Section 3 (*Evaluation; NFR*).

7.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (*Warranty*) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7.4. **Except as expressly stated in this Section 7 (Warranty), the disclaimers in Section 13 (Disclaimer of Warranties) of the General Terms apply to the Software.**

8. **Indemnification**.

8.1. Indemnification by Customer. In addition to the restrictions set out in the General Terms, Customer 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) infringement, misappropriation or violation of a copyright, trademark, trade secret, or privacy or confidentiality right by written material, images, logos or other content uploaded to the Entrust Technology through the Customer Account; (ii) 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 (iii) violation of applicable law by Customer, or Customer Data (collectively with those items in the General Terms, "Customer-Related Claims").

9. **Term and Termination.**

9.1. Term**.** Unless otherwise specified on the Order, the Offering Term for the Software will commence on the date that the Order is accepted by Entrust and, unless otherwise terminated pursuant to the Agreement, will expire on (i) the date the Trial Period or NFR Period expires; (ii) the date the subscription period set out in the Order expires; or (iii) the date the Customer ceases to use the Software in the case of a perpetual license (as applicable, the "Term").

9.2. Termination. In addition to the termination rights in the General Terms:

9.2.1. Entrust may terminate a license to Software granted under this IDE Schedule and refuse any additional Orders for Software if Customer commits a material breach of this IDE Schedule and fails to remedy such material breach within thirty (30) days after delivery of notice of the occurrence or existence of such breach or such longer period as may be agreed to in writing by Entrust.

9.2.2. Customer may terminate a perpetual license to Software granted under this IDE Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

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 Software ("**Third Party Vendor Products**"). Except as expressly stated in this IDE 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. **General.**

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

11.2. Publicity. Customer agrees that Entrust may identify Customer as a customer of the Software, and, subject to its prior review and approval of a proposed copy, Entrust may issue a press release and/or case study regarding Customer's use of the Software.

11.3. U.S. Government End-Users. Any software and documentation provided under the Agreement 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 software or 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 such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or 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 restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (*U.S. Government End-Users*) in writing.

11.4. Audit Rights**.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement, includgin, without limitation, with respect to the number of (i) copies of Software made or used by Customer; and (ii) CALs issued and used ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the price list current at the time of the audit. Customer shall pay the reasonable expenses incurred by Entrust to undertake the audit if the audit reveals either underpayment of more than 5% of the fees that should have been paid to Entrust for the audited period, or that Customer has materially failed to maintain Usage Records or provide them for inspection. In addition to the foregoing, Entrust shall also have the right to request that Customer provide a written report setting out the number of (i) copies of Software made or used by Customer; and (ii) CALs issued and used.

11.5. Professional Services. If Entrust provides any professional services and deliverables with respect to the Entrust Technology, such professional services and deliverables shall be subject to a separate agreement between Entrust and Customer, which may set out the scope and details of any professional services and deliverables, including, if and as applicable, resource specialist(s),

milestones, delivery dates, acceptance criteria, payment terms and any other information and terms related thereto.

Temporary Version: May 2024

Device Reputation

Special Terms and Conditions

These Device Reputation Special Terms and Conditions ("Device Reputation Special Terms") are attached to the Entrust Identity Enterprise Schedule ("IDE Schedule"), and contain the terms and conditions that govern access to and use of the Device Reputation Service (as defined herein). Capitalized terms not defined in Section 1 herein or elsewhere in these Device Reputation Special Terms shall have the meaning set out in the IDE Schedule. References to articles or sections herein shall be to articles or sections in these Device Reputation Special Terms unless otherwise expressly stated. Provisions in these Device Reputation Special Terms will prevail with respect to the Device Reputation Service over any conflicting provision in the IDE Schedule.

1. **DEFINITIONS.**

1.1. "Customer Application" means the application developed by Customer pursuant to the Device Fingerprint SDK License to be used to access and use the Device Reputation Service.

1.2. "Customer Data", in addition to its meaning in the IDE Schedule, with respect to the Device Reputation Service means Device Information, Risk Information, 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 licensors or 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 Fingerprint" means a set of attributes and characteristics designed to identify a Device.

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

1.7. "Device Reputation Service" means the Device Reputation Service which forms part of the Entrust Technology (if selected by Customer and approved by Entrust in an Order).

1.8. "Purpose" means authentication, and assessing risk associated with end user devices (including, without limitation, transaction, abuse, reputation, and fraud risk).

1.9. "Response" means the recommendation, including Risk Information, returned by the Device Reputation Service about a Device which has been evaluated by the Device Reputation Service.

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

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

1.12. "Device Fingerprint SDK License" means the Entrust Device Fingerprint SDK License through which Customer may obtain a license to use the Device Fingerprint software development toolkit. The Device Fingerprint SDK License is not a part of the Agreement.

1.13. "User" means any Data Subjects who owns or controls the Device and whose data is being collected through the Device Reputation Service.

2. **USE OF DEVICE REPUTATION SERVICE.**

2.1. Grant of License. Subject to Customer's compliance with the Agreement, Entrust grants to Customer, during the Device Reputation Term (as defined herein), a worldwide, non-exclusive, nontransferable, non-sub-licensable right to, all in accordance with the Documentation, the right to access and use the Device Reputation Service, for the purpose of collecting and processing Device Information and providing Responses to Customer. The foregoing right to use shall be contingent on Customer (i) paying the additional fees related to the Device Reputation Service as set out in the relevant Order; (ii) obtaining all necessary User consents to allow Entrust and its Affiliates and their respective licensors and service providers to: (a) collect and process Device Fingerprints for the Purpose; (b) make use of other internal end user identifiers for the Purpose; and (c) return the results from the processing outlined in (a) ("Results") to Customer.

2.2. Restrictions. Device Fingerprints and Results must only be used in connection with the Software and for the Purpose.

3. **CUSTOMER DATA & PRIVACY.**

3.1. Customer further grants to Entrust (or its Affiliates, and any of their respective licensors and service providers), a world-wide, limited right, during the Device Reputation Service 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 licensors and service providers) to provide Device Reputation Service in accordance with the Agreement.

3.2. Consents; Accuracy; Rights. Customer represents and warrants that, before authorizing a User to use Device Reputation Service 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 licensors and service 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 (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 Device Reputation Service 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.

3.3. 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 Device Reputation Service to Customer, and to sub-license such rights to any of Entrust's applicable licensors and service providers.

3.4. 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 Device Reputation Service, 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, Device Reputation Service and shall notify Entrust as soon as possible if it becomes aware of any unauthorized access or use of Device Reputation Service; (ii) use Device Reputation Service only for lawful purposes; (iii) not knowingly violate any law of any country with its use of Device Reputation Service; and (iv) not knowingly violate the intellectual property rights of any third party with its use of Device Reputation Service.

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

5. **TERM, TERMINATION & SUSPENSION.**

5.1. Termination or Suspension for Cause. Entrust may, at its sole discretion, suspend or terminate Customer's and/or Users' access to Device Reputation Service at any time, without advanced notice, if: (i) Entrust reasonably concludes that Customer and/or Users have conducted themselves in a way (a) that is not consistent with or violates the requirements of 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 Device Reputation Service by other Entrust customers and/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' and/or users' information or data processed by Device Reputation Service; or (iii) 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 Device Reputation Service for scheduled or emergency maintenance. Termination of these Device Reputation 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. **INDEMNITIES.**

6.1. In addition to Customer's indemnification obligations containd in the General Terms and the IDE 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) Customer or Customer's Users' unauthorized use of Device Fingerprints, Results, or the Device Reputation Service. "Customer-Related Claims" shall include, for the purposes of these Device Reputation Special Terms, the foregoing additional indemnification obligations.

SMS/VOICE VERIFICATION

SPECIAL TERMS AND CONDITIONS

These SMS/Voice Verification Special Terms and Conditions ("Database Special Terms") are attached to the Entrust Identity Enterprise Schedule ("IDE 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 IDE Schedule terms and conditions, and the General Terms. Capitalized terms not defined in Section 1 herein or elsewhere in these Database Special Terms shall have the meaning set out in the IDE Schedule. References to articles or sections herein shall be to articles or sections in these Database Special Terms unless otherwise expressly stated. Provisions in these Database Special Terms will prevail with respect to the SMS + Voice Verification Service over any conflicting provision in the IDE 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 Database Special Terms, Entrust hereby grants to Customer a non-exclusive, non-transferable right to use the Service during the term of their eligible active Identity Enterprise subscription or license. Customer may only use the SMS + Voice Verification Service with the Identity Enterprise product which Customer must have acquired from Entrust (or a Reseller). Entrust and/or its licensor's 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 Database 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 Database 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 Database 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) its 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 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 IDE 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 Database 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 Database 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 ("Database Special Terms") are attached to the IDE 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 Database Special Terms, the IDE Schedule terms and conditions, and the General Terms. Capitalized terms not defined in Section 1 herein or elsewhere in these Database Special Terms shall have the meaning set out in the IDE Schedule. References to articles or sections herein shall be to articles or sections in these Database Special Terms unless otherwise expressly stated. Provisions in these Database Special Terms will prevail with respect to the Databases over any conflicting provision in the IDE 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 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 Identity Enterprise subscription or license. Customer may only use the GeoIP Databases with the Identity Enterprise product which Customer must have acquired from Entrust (or a Reseller). Entrust and/or its licensor's 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 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 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 Identity Enterprise;

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 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 Identity Enterprise subscription or license (or termination of Customer's entitlement to the GeoIP Databases).

4. **WARRANTY DISCLAIMER.**

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