



Identity Essentials

End User License Terms and Conditions

The Agreement for Entrust's Identity Essentials Offering ("Identity Essentials") is made up of these end user license terms and conditions (the "Identity Essentials Schedule"), the Entrust General Terms and Conditions available at <https://www.entrust.com/general-terms.pdf> ("General Terms"), and an Order for Identity Essentials. 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. "Authentication Client" means one of the following Software components responsible for authentication for a specific type of client (as further described in the Documentation): Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection, Windows Logon Protection, or Secure Device Provisioning.
- 1.2. "Cloud Setup" has the meaning set out in Section 2.16 (*Cloud Setup*).
- 1.3. "Component" means one or more of the following Software components (as further described in the Documentation): Database Service, Web Administration Interface, Self-service Website, Transmitter Service, Authentication Backend Service, PowerShell Support.
- 1.4. "Computer" means a single physical hardware system with an internal storage device capable of running the Software (e.g., a single personal computer, workstation, terminal, hand held computer, pager, telephone, personal digital assistant, server or other single electronic device).
- 1.5. "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 Software. Customer Data may include Personal Data.
- 1.6. "Customer Subscription License Program" means the program under which Customer can purchase licenses for the Software for its own internal business purposes on a subscription basis for the Customer Subscription Period.
- 1.7. "Customer Subscription Period" has the meaning set out in Section 2.3.2 (*Customer Subscription License Program*).
- 1.8. "Database Service Component" means the service responsible for storing the Software user data and configuration data.
- 1.9. "Data Subjects" shall have the meaning set out in the DPA.



- 1.10. "Direct Support Services" means the support services for the Software, provided directly by Entrust to Customer and either included as part of Customer's selected license program, or otherwise subject to additional fees. Direct Support Services are further described in the Documentation, and expressly exclude Indirect Support Services which are provided by Resellers.
- 1.11. "Dispatch License" means the license required for each modem, email connector or dispatch connector created in the Database Service Component, as further detailed in the Documentation.
- 1.12. "Documentation" means written materials prepared by Entrust (or its licensors or service providers) relating to the Software, 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 Software, all as may be modified from time to time.
- 1.13. "Entrust Technology" means the Software and the Documentation.
- 1.14. "Hybrid Setup" means Customer's on-premise installation of the Components and Authentication Clients, and configuration of the Database Service Component and Authentication Backend Service Component to communicate with Identity as a Service.
- 1.15. "Identity as a Service" means Entrust's Identity as a Service cloud-based platform.
- 1.16. "Identity as a Service Terms of Service" means the Identity as a Service standard terms of service, as may be updated from time to time, located at <https://www.entrust.com/-/media/documentation/licensingandagreements/identity-as-a-service-schedule.pdf>.
- 1.17. "Identity Mobile App" means the Entrust Identity Mobile application available for iOS and Android mobile devices (i) that enables mobile devices to receive messages sent by the Software, (ii) that is downloaded, installed and used by Users on their mobile devices, and (iii) that is subject to a separate end user license agreement to be agreed to by the User downloading, installing and/or using the application.
- 1.18. "Indirect Support Services" means the support services for the Software that Customer may purchase and receive directly from a Reseller. Indirect Support Services are not covered by the Agreement.
- 1.19. "License Key" means a unique set of numbers, characters and/or symbols issued by Entrust and sent to Customer in the license email to enable Customer to unlock the Software during installation.
- 1.20. "MFA CAL" means the client access license that must be assigned to a User authorized to access a system that has been protected by the Software and must only be utilized within a single instance of the Database Service Component.
- 1.21. "On-premise Setup" means Customer's on-premise installation of the Software, without configuration of the Database Service Component and Authentication Backend Service Component to communicate with Identity as a Service.
- 1.22. "Open License Program" means the particular Service Provider License Program as further described in the Documentation under which Service Provider can purchase licenses for the Software on a per user, per calendar month subscription basis.
- 1.23. "Password Reset CAL" means the client access license that must be assigned to an individual user allowed to access the optional Identity Essentials password reset component and which may



only be utilized within a single instance of the Database Service Component.

- 1.24. "Perpetual License Program" means the program under which eligible Customers can purchase licenses for the Software for its internal business usage on a perpetual basis.
- 1.25. "Reseller" means a legal entity that has entered into a valid agreement with Entrust or an Entrust authorized distributor to resell to Customer the Software licenses and, if applicable, Software Assurance Services and Direct Support Services. Reseller may also be authorized to provide Indirect Support Services.
- 1.26. "Service Provider" means a Customer that is a hosting provider or service provider that offers hosting infrastructure and/or business applications to its Tenants (and their respective Users) and meets the requirements of the Service Provider License Program and, as applicable, the requirements of the Open License Program.
- 1.27. "Service Provider License Period" has the meaning set out in Sections 2.3.3 (*Service Provider License Program (excl.. Open License Program)*) and 2.3.4 (*Service Provider Under Open License Program*), as applicable.
- 1.28. "Service Provider License Program" means the program under which a Service Provider can purchase licenses for the Software during the Service Provider License Period for the purpose of providing an authentication service and/or password reset service to its Tenants and their Users.
- 1.29. "Software" means Entrust's Identity Essentials computer software product in machine-readable object code form (excluding any Ancillary Software), including, without limitation, the Components, the Authentication Clients, and any Updates and/or Upgrades to which Customer is entitled.
- 1.30. "Software Assurance Services" means the services available to Customer under the Perpetual License Program for optional purchase as further detailed in Section 2.11 (*Software Assurance*).
- 1.31. "Special Terms and Conditions" mean any terms and conditions attached to this Identity Essentials Schedule.
- 1.32. "Starter Pack" means a collection of types of licenses (e.g., MFA CALs, Password Reset CALs and Dispatch Licenses) that are bundled into a commercial package.
- 1.33. "Tenant" means any Service Provider customer or client that has entered into a Tenant Agreement (as such term is defined in Section 2.4.6) through which such customer or client has accepted the terms and conditions of this Agreement.
- 1.34. "Trial Software" means Software licensed to Customer for purposes of internal evaluation only for the Trial Period subject to the terms and conditions of this Agreement.
- 1.35. "Trial Period" means the term as specified in the license email sent to Customer, or, if not specified, thirty (30) days.
- 1.36. "Upgrade Entitlement" a right for a Customer to get access to Updates (as defined below) and/or Upgrades (as defined below).
- 1.37. "Update" means minor new software product functionality or code that incorporates all previous fixes and service packs (if any exist) since the last Update of the Software and made generally available by Entrust. An Update is tied to the preceding version and is typically designated by a number to the right of the decimal point such as 1.1, 1.2, 1.3, etc.
- 1.38. "Upgrade" means major changes in software product functionality or code that incorporates the



previous release (if one has occurred), fixes and service packs (if they have occurred) and made generally available by Entrust. An Upgrade is designated by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc.

1.39. "User" means any individual end user who is authenticated by Customer or a Tenant (if Customer is a Service Provider) using the Software.

2. **Software Licenses.**

2.1. **Grant of License.** Subject to the terms and conditions stated in this Agreement, Entrust grants Customer a limited, non-exclusive, non-transferable license to install and use the Software (On-premise Setup and Hybrid Setup only), subject to the following limitations:

2.1.1. Use of the Software is limited to the quantity of Dispatch Licenses, MFA CALs and Password Reset CALs purchased by Customer under this Agreement as stated in the license email that Customer receives following the purchase of a Software license;

2.1.2. Use of the Software is limited to the features and functionalities that Customer is licensed to use and/or purpose for which the Software is designed as described in the applicable Documentation;

2.1.3. Except for perpetual licenses (granted under the Perpetual License Program), all licenses are limited in duration as defined by the applicable license program (see Section 2.3 (*License Programs*));

2.1.4. Customer shall only use the License Key in conjunction with the copy of Software for which it was delivered, and Customer cannot copy or alter the License Key;

2.1.5. Customer must comply with any and all technical limitations in the Software that only allow Customer to use Software in specific ways;

2.1.6. Subject to any license program-specific exceptions expressly set out in Section 2.3 (*License Programs*), irrespective of the number of MFA CALs or Password Reset CALs granted by Entrust, the license to the Software only covers the installation of the Database Service Component on a single Computer, and only for Customer's internal business use, and Customer is not allowed to have more than one installation of the Database Service Component running at any point of time. If the Database Service Component is relocated to a different Computer, Customer must remove the Database Service Component from the former Computer;

2.1.7. Customer is required to comply with any license program requirements set forth in the applicable Documentation or otherwise made available to Customer by Entrust;

2.1.8. Customer is solely responsible for determining whether the Software is sufficient for its purposes, including but not limited to whether the Software satisfies Customer's legal and/or regulatory requirements (or those of its Tenants or Users);

2.1.9. Customer is responsible and liable for the configuration of the Software to meet its own (and its Tenants' and/or Users') requirements;

2.1.10. Entrust's relationship is with Customer and not its Tenants (if Customer is a Service Provider) and/or Users. Customer acknowledges and agrees that it shall be responsible for coordinating all communication with Entrust under this Agreement, and that Entrust shall direct any requests or other communications by Tenants or Users to Customer; and

2.1.11. Customer is allowed to make a backup copy of the Software. Customer may use such copy only to reinstall the Software.

2.2. License Types. There are three different types of licenses available for the Software (On-premise Setup and Hybrid Setup only) as further described in the applicable Documentation. They are as follows: (a) Dispatch Licenses; (b) MFA CALs; and (c) Password Reset CALs. Customer may have a mandatory minimum number of such licenses it must purchase for the Software, and additional specific license-type requirements and entitlements may apply depending on Customer's choice of license program, and as set out in the applicable Documentation. For example, for some license programs it is mandatory for Customer to purchase a Starter Pack initially. A single default dispatch connector is automatically created by the system and is licensed hereunder for use for sending messages via a specific cloud service to the Identity Mobile App. Additionally, for Customers on a Customer Subscription License Program such default dispatch connector can be used to send SMS and voice call messages (ten (10) SMSs per user per month (unless other amount agreed to in writing by Entrust) at no charge – related to Software). This default dispatch connector does not require a Dispatch License.

2.3. License Programs. There are a number of license programs available for the Software (On-premise Setup and Hybrid Setup only), as follows:

2.3.1. *Perpetual License Program*. A Customer under the Perpetual License Program is granted a perpetual license to the Software (subject to the termination provisions in this Agreement). Customer is not eligible to receive (i) the Upgrade Entitlement or Direct Support Services, (ii) access to the Identity Mobile App for its Users, or (iii) access to the geofencing functionality of the Software, unless Customer has purchased these separately under the Software Assurance Services.

2.3.2. *Customer Subscription License Program*. A Customer under the Customer Subscription License Program is granted a subscription-based license for the Software for the Customer Subscription Period (which means the term for which Customer has purchased licenses under the Customer Subscription License Program as specified in the license email sent to Customer). If Customer elects to renew its subscription, the Customer Subscription Period will be extended to include the term of the renewal, subject to Customer paying the applicable renewal fees within the prescribed period. It is Customer's responsibility to renew its subscription prior to expiration to avoid downtime of the Software. During the Customer Subscription Period, Customer possesses the Upgrade Entitlement and is eligible for Direct Support Services in accordance with the applicable Documentation.

2.3.3. *Service Provider License Program (excl.. Open License Program)*. A Service Provider under the Service Provider License Program is granted a subscription-based license for the Service Provider License Period (which means the length of time for which Service Provider has purchased licenses for the Software as specified in the license email sent to Service Provider). If Service Provider elects to renew its subscription, the Service Provider License Period will be extended to include the term of the renewal, subject to Service Provider paying the applicable renewal fees within the prescribed period. It is the Service Provider's responsibility to renew its subscription prior to expiration to avoid downtime of the Software. During the Service Provider License Period, Service Provider possesses the Upgrade Entitlement and is eligible for Direct Support Services in accordance with the applicable Documentation.

2.3.4. *Service Provider Under Open License Program*. A Service Provider under the Open License Program is granted a subscription-based license for the Service Provider License Period (which means a one (1) calendar month period, with the exception that if the initial term commences after the first day of any calendar month then the initial Service Provider License Period will only be the remainder of such calendar month). The subscription automatically renews for one (1) calendar month consecutive terms and the Service Provider License

Period will be extended to include the term of the renewal, subject to Service Provider paying the applicable renewal fees within the prescribed period. Service Provider is required to provide at least one (1) month prior written notice to Entrust (directly or through its Reseller) if Service Provider wishes to terminate its participation in the Open License Program and must stop using the Software at the end of such one (1) month period (invoicing of any usage will continue if Service Provider continues to use the Software). If payment is not received by Entrust for a given monthly subscription period within the prescribed period, the Service Provider License Period immediately ends at the end of the next month and Service Provider must stop using the Software and immediately pay all amounts due. Notwithstanding the restrictions stated in Sections 2.1.6 and 2.1.7, a Service Provider granted licenses under the Open License Program is allowed to have more than one installation of the Database Service Component running, but will be invoiced for each such installation based on the assigned CALs in each Database Service Component. Each Database Service Component will automatically report the actual CAL assignments to Entrust on a periodic basis. In cases where the automatic reporting activity generated by the Software fails during a period of more than thirty (30) consecutive days, the Software will automatically limit the available functionality of the Software until such reporting activity has been restored. Service Provider is responsible for paying for all CAL assignments even if not reported. During the Service Provider License Period, Service Provider possesses the Upgrade Entitlement and is eligible for Direct Support Services in accordance with the Documentation.

2.4. Additional Terms for Service Providers.

- 2.4.1. Any additional terms and conditions that are either set forth in the Identity Essentials Open License Program Documentation, or, to the extent incorporated herein by reference and made available on Entrust's website or as otherwise provided by Entrust to Customer, shall apply to Service Provider;
- 2.4.2. With respect to the Service Provider License Program (or Open License Program), the Service Provider hereby expressly agrees that Service Provider is liable and responsible for its Tenants and Users, and their compliance with the terms and conditions of this Agreement. A breach by any such Tenant or User of the terms and conditions of this Agreement shall be considered to be a breach by and the responsibility of the Service Provider. Service Provider will indemnify, defend and hold harmless Entrust Group 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 Service Provider's participation in the Service Provider License Program, use of the services or Software by Tenants and/or Users, and any dispute between Service Provider and its Tenants and/or Users;
- 2.4.3. Additional terms and conditions may apply to Service Providers as set out in the Service Provider License Program (or Open License Program). In case there is a conflict between the terms and conditions stated in this Agreement and terms and conditions under the Service Provider License Program, this Agreement prevails;
- 2.4.4. Service Provider will make no representations or warranties regarding the Software or any other matter (including without limitation Identity as a Service), to Tenants, Users, and/or any other third party, for or on behalf of Entrust, and Service Provider will not create or purport to create any obligations or liabilities on or for Entrust regarding the Software or any other matter (including, without limitation, Identity as a Service). Service Provider will be liable to Entrust for any and all Tenants' and/or Users' acts and/or omissions in relation to or breach of this Agreement;
- 2.4.5. Entrust is not responsible for, and disclaims all liability with respect to Tenants and/or Users; and

- 2.4.6. Service Provider shall enter into a tenant agreement with each of its Tenants which will be at least as protective of Entrust (and its Affiliates, licensors, suppliers and hosting providers) and the Software as this Agreement (the "Tenant Agreement"). Without limiting the generality of the foregoing, the Tenant Agreement will: (i) not contain any representation or warranty on behalf of Entrust or create or purport to create any obligation or liability on Entrust; (ii) disclaim any and all liability on behalf of Entrust; (iii) name Entrust as an indemnified party in any indemnification obligation benefiting Service Provider; (iv) provide for rights of termination consistent with those contained in this Agreement; and (v) make Entrust third party beneficiaries to the clauses implementing (ii), (iii) and (iv) above; (vi) provide appropriate notices to Users and obtain from the Users all necessary consents required for Service Provider to meet its obligations to Entrust under this Agreement; and (vii) in any reference to "Entrust", also cover Entrust's Affiliates, licensors, suppliers and hosting service providers.
- 2.5. 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.
- 2.6. Updates and Upgrades. To install and/or use Updates and/or Upgrades to the Software, Customer must first be licensed for the version of Software that is eligible for the Update/Upgrade. Upon Upgrade and/or Update, the agreement that accompanies the Upgrade and/or Update will take the place of the agreement for the version of the Software from which Customer upgraded and/or updated. When Customer has upgraded and/or updated the Software, Customer may no longer use the Software or previous versions of the Software, from which Customer upgraded and/or updated. If no agreement accompanies the Update and/or Upgrade to the Software, then the last version of the agreement that accompanied the Software will apply.
- 2.7. 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.
- 2.7.1. Work around any technical limitations in the Software;
- 2.7.2. Reverse engineer, translate, decompile or disassemble the Software or in any other manner decode the Software except to the extent that the foregoing restriction is expressly prohibited by applicable law notwithstanding a contractual obligation to the contrary;
- 2.7.3. Create a subset, superset or other derivative of the Software or any portion thereof;
- 2.7.4. Make more copies of the Software than expressly specified in this Agreement;
- 2.7.5. Host, time-share, sell, publish, rent, lease, lend, distribute, license, sublicense, transfer, assign, encumber, grant a security interest in, or otherwise transfer the Software;
- 2.7.6. Use nor have the right to use the Software as a service bureau or as any other hosted service for or on behalf of any third party;
- 2.7.7. Make the Software available for use by third parties, unless Customer is a Service Provider enrolled under the Service Provider License Program (and in that case subject to the restrictions set out in this Agreement with respect to such license program);
- 2.7.8. Make any modifications, adaptations or changes to the Software without the express written permission of Entrust; and

2.7.9. Remove, modify or alter any of Entrust's copyright, trademark or proprietary rights notices from any part of the Software (including notices on physical media).

The restrictions on Customer with respect to the Software as set forth in Sections 2.7.3, 2.7.4, 2.7.7, 2.7.8, and 2.7.9 above also apply to the Documentation.

- 2.8. 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.
- 2.9. Documentation. Customer is also granted the right to use for internal business use and to make a reasonable number of copies of any Documentation made available to Customer by Entrust (i) for the purpose of using, installing, and troubleshooting the Software during the term of the Software license, (ii) for the purpose of complying with the terms and conditions of this Agreement, or (iii) for the purpose of using the Direct Support Services or Software Assurance Services during the term of such Direct Support Services or Software Assurance Services, as applicable.
- 2.10. Direct Support Services. Subject to the terms and conditions of this Agreement and the Documentation, the Direct Support Services may be provided by Entrust to Customer on an annual basis. After a period of twelve (12) months, Customer may renew the Direct Support Services as set out in the Documentation. Notwithstanding the foregoing, where support is purchased through a Reseller and the relevant order indicates that the Reseller will provide support, then such support constitute Indirect Support Services. Entrust will have no obligation to provide support or other services directly to Users. Support for certain third party products, if made available by Entrust and purchased by Customer, shall be provided pursuant to separate terms and conditions.
- 2.11. Software Assurance. Software Assurance Services is an optional service that Customers under the Perpetual License Program can purchase in order to get the Upgrade Entitlement for a prescribed period. This gives Customer the entitlement to receive new Updates and Upgrades to the Software as such are made generally available to Customers from Entrust, provided that Customer has purchased Software Assurance Services. Software Assurance Services also entitles Customers to (i) access the Identity Mobile App for its Users, or (ii) access the geofencing functionality of the Software. Customer's Software Assurance Services must be active at the time when the relevant Updates and/or Upgrades to the Software are made generally available to Customers, or at the time Customer (or its Users) access the Identity Mobile App or the geofencing functionality of the Software. Software Assurance Services do not include Direct Support Services. Customer is only entitled to Software Assurance Services if ordered and paid for by Customer. Software Assurance Services will not include any releases of the Software that Entrust, at its sole discretion, determines to be a separate product, or for which Entrust charges its Customers extra or separately. The terms of this Agreement and the additional terms set forth in the Software Assurance Services Documentation (or otherwise made available by Entrust to Customer) apply to the Software Assurance Services unless a new end-user-license agreement between Entrust and Customer replaces this Agreement.
- 2.12. 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.
- 2.13. 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, Tenants, and/or Users, by text messages or by any other means through the Identity Essentials 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 Group 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.

- 2.14. 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.
- 2.15. Use and Access to Identity as a Service (Hybrid Set Up only). Customer will be provided with limited access to and use of Identity as a Service, subject to the following requirements and restrictions:
- 2.15.1. Access to and use of Identity as a Service is included in Customer’s Software license granted under this Agreement;
- 2.15.2. Customer must click-through and agree to the Identity as a Service Terms of Service, and such terms and conditions shall apply to Customer’s use of the Identity as a Service features and functionality, subject to the additional rights and restrictions set out in this Section 2.15 (*Use and Access to Identity as a Service (Hybrid Set Up only)*) or as otherwise set out in the Documentation;
- 2.15.3. Identity as a Service (as integrated with the Software) is currently supported by the following Authentication Clients: RADIUS Protection, AD FS Protection, IIS Website Protection, and Windows Logon Protection (other Authentication Clients do not currently support Identity as a Service) and Customer shall only be permitted to use such Authentication Clients with Identity as a Service;
- 2.15.4. Customer under the Perpetual License Program (standard or not-for-resale/NFR) for the Software: (i) must have a valid, fully paid-up entitlement to Software Assurance Services, (ii) will only have access to push authentication, email one-time password (OTP), token OTP, temporary access code, and device finger print functionality (as such terms are further detailed in the Identity as a Service documentation), and (iii) will not be entitled to use SMS dispatching and voice OTP from Identity as a Service;
- 2.15.5. Customer under the Customer Subscription License Program must have a valid and fully paid-up subscription. Customer will (i) get access to the Identity as a Service Plus Bundle (as further detailed in the Identity as a Service documentation), and (ii) notwithstanding the description in the Identity as a Service Plus Bundle, get twenty (20) SMSs per user per year at no charge (related to Identity as a Service);
- 2.15.6. Customer under a Service Provider License Program (standard or Open License Program) must have a valid and fully paid-up subscription. Customer will get access to the Identity as a Service Plus Bundle (as further detailed in the Identity as a Service documentation), but will not be entitled to use SMS dispatching and voice OTP from Identity as a Service without prior



written permission (which may include additional charges);

2.15.7. In the event of conflict between the Identity as a Service Terms of Service and this Agreement, with respect to Identity as a Service and its features and functionality, the terms and conditions of the Identity as a Service Terms of Service shall prevail to the extent of the conflict.

2.16. Cloud Setup. "Cloud Setup" refers to any instance where Customer's use of Identity as a Service is solely based on the Identity as a Service Terms of Service and where Customer's right of access to and use of Identity as a Service is not subject to any license obtained pursuant to this Agreement (including any related additional rights or restrictions). With respect to the Cloud Setup the following also applies:

2.16.1. RADIUS Protection, AD FS Protection, IIS Website Protection, and Windows Logon Protection Authentication Clients are also covered (licensed) under the Identity as a Service Terms of Service; and

2.16.2. In the event Customer obtained rights to access and use Identity as a Service pursuant to this Agreement, such rights shall automatically expire to the extent any of the requirements set out in Section 2.16 (*Use and Access to Identity as a Service (Hybrid Set Up only)*) are no longer met. Thereafter, any subsequent use of Identity as a Service shall be solely pursuant to the Identity as a Service Terms of Service.

3. Trial License.

3.1. If Customer has received Trial Software, regardless of how it is labelled, the license to use the Trial Software is limited in time to the Trial Period. The terms of this entire Agreement will also apply to Customer's use of Trial Software subject to the following specific overriding terms and conditions:

3.1.1. Grant of License. Entrust grants Customer a limited, non-exclusive license to use the Trial Software for the sole purpose of evaluating the Trial Software's suitability for Customer's internal business requirements. The license granted is limited in time to the Trial Period.

3.1.2. Termination. Upon notice to Customer, Entrust can terminate this license to the Trial Software with immediate effect at any time. Furthermore, the license to the Trial Software will automatically terminate without notice on the earlier of: expiration of the Trial Period, or Customer's completion of its evaluation of the Trial Software.

3.1.3. Limited Software. Parts (or functionality) of the full version of the Software may be withheld or unusable to Customer of the Trial Software.

3.1.4. As Is. Trial Software is provided to Customer AS IS without any warranties, rights to remedies or liabilities, indemnities, or support services being provided by Entrust.

4. Fees.

4.1. Customer will pay the costs and fees (including where overages are applicable, any overage fees) for the Software 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 provides for a period of ninety (90) days from the date of delivery of the initial Software product a right of remedy as a result of such Software not performing in substantial accordance with the Documentation delivered with such Software consisting of, at Entrust’s option, (i) repairing or replacing such Software which is returned to Entrust, or (ii) taking return of such Software and refunding the price paid for such Software. Customer must make a valid claim for such remedy and demonstrate that the Software does not perform as set forth above within the ninety (90) days. Entrust will 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 Entrust. For greater certainty, there is no right of remedy for Updates and/or Upgrades. Entrust further warrants that 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 program, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the use of computer and telecommunications software or hardware for their normal purposes.
- 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.** EXCEPT AS SPECIFICALLY STATED HEREIN, ENTRUST’S EXCLUSIVE LIABILITY AND CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR ANY DEFECT OR DELAY SHALL BE SUBJECT TO THE LIMITATION ON AND EXCLUSION OF DAMAGES SET OUT BELOW. THESE LIMITATIONS AND EXCLUSIONS APPLY EVEN IF REPAIR, REPLACEMENT OR A REFUND FOR THE SOFTWARE DOES NOT FULLY COMPENSATE THE CUSTOMER FOR ANY LOSSES; OR ENTRUST KNEW OR SHOULD HAVE KNOWN ABOUT THE POSSIBILITY OF THE DAMAGES. TO THE MAXIMUM EXTENT

PERMITTED BY LAW, EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMENT, THE SOFTWARE AND ANY RELATED SERVICES ARE PROVIDED “AS IS”, WITHOUT ANY REPRESENTATIONS, CONDITIONS, OR WARRANTIES OF ANY KIND. WITHOUT LIMITATION, ENTRUST, INCLUDING ITS AFFILIATES, LICENSORS, SUBCONTRACTORS, DISTRIBUTORS, SUPPLIERS, OR AGENTS, AND THEIR RESPECTIVE DIRECTORS, OFFICERS OR EMPLOYEES (COLLECTIVELY, THE “ENTRUST GROUP”), DISCLAIMS ALL OTHER REPRESENTATIONS, WARRANTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT AS OTHERWISE PROVIDED IN THIS AGREEMENT, THE ENTIRE RISK OF THE USE OF THE SOFTWARE OR RECEIPT OF ANY RELATED SERVICES HEREUNDER SHALL BE BORNE BY CUSTOMER. FURTHERMORE, ENTRUST GROUP DOES NOT REPRESENT NOR WARRANT THAT THE SOFTWARE OR ANY RELATED SERVICES WILL: ACHIEVE SPECIFIC RESULTS, OPERATE WITHOUT INTERRUPTION, DISPLAY CORRECT INFORMATION ABOUT A USER’S LOCATION AND/OR ORGANIZATION (SINCE SOME INFORMATION IS RECEIVED FROM THIRD PARTIES), BE ERROR FREE, OR BE ABSOLUTELY IMPENETRABLE TO HACKERS WILFULLY TRYING TO GAIN ACCESS TO THE CUSTOMER’S COMPUTER SYSTEM. INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE.

7.4. **Except as expressly stated in 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; (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.** The Agreement will commence upon Customer’s acceptance of the Agreement and, unless otherwise terminated pursuant to the Agreement, will expire on (i) the date the Trial Period expires; or (ii) for so long as Customer continues 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 Identity Essentials Schedule and refuse any additional Orders for Software if Customer commits a material breach of this Identity Essentials 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 Identity Essentials 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 Identity Essentials 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 between this Identity Essentials Schedule and Special Terms and Conditions, the latter 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, including, 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 Software, 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.
- 11.6. Third Party Services. Customer's use of third party products or services (including, without limitation, SMS message delivery services) that are not licensed to Customer directly by Entrust ("Third Party Services") will be governed solely by the terms and conditions applicable to such Third Party Services, as agreed to between Customer and the relevant third party. Entrust does not endorse or support, is not responsible for, and disclaims all liability with respect to Third Party Services, including, without limitation, the privacy practices, data security processes or other policies and practices of the relevant third party. Customer agrees to waive any and all claims against Entrust with respect to any Third Party Services.

Template Version: August 2023



SMS/VOICE VERIFICATION

SPECIAL TERMS AND CONDITIONS

These SMS/Voice Verification Special Terms and Conditions (“SMS + Voice Special Terms”) are attached to the Identity Essentials 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 Identity Essentials Schedule terms and conditions, and the General Terms. Capitalized terms not defined in Section 1 herein or elsewhere in these SMS + Voice Special Terms shall have the meaning set out in the Identity Essentials Schedule. References to articles or sections herein shall be to articles or sections in these SMS + Voice Special Terms unless otherwise expressly stated. Provisions in these SMS + Voice Special Terms will prevail with respect to the SMS + Voice Verification Service over any conflicting provision in the Identity Essentials 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 SMS + Voice 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 Essential subscription or license. Customer may only use the SMS + Voice Verification Service with the Identity Essentials 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 SMS + Voice 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 SMS + Voice 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 SMS + Voice 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. Section 2.13 (*Content of Text Messages (SMS); E-Mails, Etc.*) of the Identity Essentials Schedule shall also apply to the SMS + Voice Verification Service.

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 9.2 (*Indemnification by Customer*) of these SMS + Voice Special Terms, 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 4.2.3. "Customer-Related Claims" shall include, for the purposes of these SMS + Voice 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 SMS + Voice 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.