ENTRUST IDENTITY AS A SERVICE ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") describes rules that apply to any party that uses the Entrust Identity as a Service cloud-based authentication platform (the "**Service**"). The prohibited conduct in this AUP is not exhaustive. This AUP is incorporated by reference into and governed by the Entrust Identity as a Service Terms of Service, the Entrust Identity as a Service Terms of Service (MSP Model), or other similar written agreement between you (individually and collectively the "Customer" or "MSP", hereinafter referred to as "**You**" and "**Your**") and the Entrust entity with which You entered into such agreement (the "**Agreement**") covering the Service. By using the Service, You agree to the latest version of this AUP. If You violate the AUP or authorize, encourage, or help others (including any of Your users) to do so, we may suspend or terminate Your use of the Service (including that of any of Your users).

This AUP may be updated by Entrust from time to time upon reasonable notice, which may be provided via Your account, e-mail, or by posting an updated version of this AUP at https://www.entrust.com/-/media/documentation/licensingandagreements/identity-as-a-service-acceptable-use-policy.pdf.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate, or instruct others to use, the Service:

(i) for any illegal, deceptive, harmful, fraudulent, infringing, abusive or offensive use, or for any other activities that materially interfere with the business or activities of Entrust; (ii) to threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm; (iii) for any content or activity that promotes child sexual exploitation or abuse; (iv) to violate the rights of others; (v) in violation of laws, regulations, governmental orders, industry standards, or telecommunications providers' requirements or guidance in any applicable jurisdiction, including any of the foregoing that require (a) consent be obtained prior to transmitting, recording, collecting, or monitoring data or communications or (b) compliance with opt-out requests for any data or communications; (vi) to transmit, store, display, distribute or otherwise make available content or communications (commercial or otherwise) that are illegal, deceptive, harmful, unwanted, inappropriate, fraudulent, objectionable, infringing, offensive, including, but not limited to, content or communications which Entrust determines (a) are false or inaccurate; (b) are hateful or encourages hatred or violence against individuals or groups; or (c) could endanger public safety. These prohibitions include use of the Service by a hate group.

No Security Violations

You may not use the Service to violate the security, integrity, or availability of any network, computer or communications system, software application, or network or computing device, including, without limitation, the computers used to provide the Service. Prohibited activities include:

- **Unauthorized Access**. Accessing, attempting to access, or using the Service without permission or authorization, including probing, scanning, finding, testing for security vulnerabilities to exploit the Service or to breach or bypass any security or authentication measures, security mechanisms, or filtering capabilities used by the Service. The foregoing shall include all attempts to carry out such activities, whether successful or not, as well as attempting to access or otherwise interfere with the accounts of customers and/or users of the Service.

- **Interception**. Monitoring of data or traffic on the Service without permission.

- **Falsification of Identity or Origin**. Creating a false identity or any attempt to mislead others as to the

identity of the sender or the origin of any data or communications.

No Network Abuse

You may not make network connections to any users, hosts, or networks unless You have permission to communicate with them. Prohibited activities include:

- **Interference with the Service**. Interfering with or otherwise negatively impacting any aspect of the Service or any third-party networks that are linked to the Service. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

- **Monitoring or Crawling**. Monitoring or crawling of the Service that impairs or disrupts the Service being monitored or crawled.

- **Disabling the Service**. Any denial of service (DoS) attack on the Service or any other conduct that attempts to disrupt, disable, or overload the Service.

- **Computer Viruses**. Do not intentionally distribute or transmit code, files, scripts, agents, or programs intended to do harm, including viruses or malware, or using automated means, such as bots or in any other way attempt to gain access to or interfere with the functioning of any computer, communications system, or website, including the computer, and communications systems used to provide the Service.

- **Operation of Certain Network Services**. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

- **Avoiding System Restrictions or Security Mechanisms**. Using manual or electronic means to avoid, bypass or break any use limitations placed on a System, such as access and storage restrictions, or otherwise attempting to penetrate or disable any security system or mechanisms. Using the Service in any other manner that poses a material security or service risk to Entrust or any of its other customers. Reverse-engineering the Service in order to find limitations, vulnerabilities, or evade filtering capabilities.

No E-Mail or Other Message Abuse

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this AUP or the acceptable use policy of that provider. Engaging in any unsolicited advertising, marketing or other activities prohibited by applicable law or regulation covering anti-spam, data protection, or privacy legislation in any applicable jurisdiction, including, but not limited to anti-spam laws and regulations such as the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act. Using the Service in connection with unsolicited, unwanted, or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video, or faxes.

Messaging

Consent/Opt-in

What Is Proper Consent?

Consent can't be bought, sold, or exchanged. For example, You can't obtain the consent of message recipients by purchasing a phone list from another party.

Aside from two exceptions noted later in this section, You need to meet each of the consent requirements listed below. You need to require that Your customers adhere to these same requirements when dealing with their users and customers.

Consent Requirements

- Prior to sending the first message, You must obtain agreement from the message recipient to communicate with them - this is referred to as "consent", You must make clear to the individual they are agreeing to receive messages of the type you're going to send. You need to keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow.

- If You do not send an initial message to that individual within a reasonable period after receiving consent (or as set forth by local regulations or best practices), then You will need to reconfirm consent in the first message you send to that recipient.

- The consent applies only to You, and to the specific use or campaign that the recipient has consented to. You cannot treat it as blanket consent allowing You to send messages from other brands or companies You may have, or additional messages about other uses or campaigns.

- Proof of opt-in consent should be retained as set forth by local regulation or best practices after the end user opts out of receiving messages.

Alternative Consent Requirements

While consent is always required and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.

Contact initiated by an individual

If an individual sends a message to You, You are free to respond in an exchange with that individual. For example, if an individual texts Your phone number asking for Your hours of operation, You can respond directly to that individual, relaying Your open hours. In such a case, the individual's inbound message to You constitutes both consent and proof of consent. Remember that the consent is limited only to that particular conversation. Unless You obtain additional consent, don't send messages that are outside that conversation.

Informational content to an individual based on a prior relationship

You may send a message to an individual where You have a prior relationship, provided that individual provided their phone number to You, and has taken some action to trigger the potential communication and has not expressed a preference to not receive messages from You. Actions can include a button press,

alert setup, appointments, or order placements. Examples of acceptable messages in these scenarios include appointment reminders, receipts, **one-time passwords (OTP)**, order/shipping/reservation confirmations, drivers coordinating pick up locations with riders, and repair persons confirming service call times.

The message cannot attempt to promote a product, convince someone to buy something, or advocate for a social cause.

Periodic Messages and Ongoing Consent

If You intend to send messages to a recipient on an ongoing basis, You should confirm the recipient's consent by offering them a clear reminder of how to unsubscribe from those messages using standard opt-out language (defined below). You must also respect the message recipient's preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent as set forth by local regulations and best practices.

Identifying Yourself as the Sender

Every message You send must clearly identify You (the party that obtained the opt-in from the recipient) as the sender, except in follow-up messages of an ongoing conversation.

Opt-out

The initial message that You send to an individual needs to include the following language: "Reply STOP to unsubscribe," or the equivalent using another standard opt-out keyword, such as STOPALL, UNSUBSCRIBE, CANCEL, END, and QUIT.

Individuals must have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, You may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before You can send any additional messages.

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any suspected violation of this AUP or misuse of the Service. We may (i) investigate violations of this AUP or misuse of the Service; or (ii) remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with You for use of the Service.

You agree to cooperate with us to remedy any violation. When determining whether there has been a violation of this AUP, we may consider your ability and willingness to comply with this AUP, including the policies and processes you have in place to prevent or identify and remove any prohibited content or activity.

Reporting of Violations of this AUP

If You become aware of any violation of this AUP, including any prohibited content or communications, You will immediately notify us and provide us with cooperation, as requested by us, to investigate, stop, or remedy, the violation. To report any violation of this AUP, please follow our abuse reporting process.