ENTRUST IDENTITY AS A SERVICE ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") describes actions that Entrust prohibits when any party uses the Entrust Identity as a Service cloud-based authentication platform (the "**Service**"). The examples described in this AUP are not exhaustive. This AUP is incorporated by reference into, and governed by the Entrust Identity as a Service Terms of Service or other similar written agreement between you (individually and collectively the "Customer", "MSP", and/or "Tenant", hereinafter referred to as "**You**" and "**Your**") and the Entrust entity with which You entered into such agreement (the "**Agreement**"). References to "Entrust" shall also include, in addition to the Entrust contracting entity, its affiliates, subsidiaries, licensors, and other service providers. The Agreement contains definitions of capitalized terms not otherwise defined in this AUP (e.g. "Service", "Customer", "MSP", "Tenant", and "Agreement") and such definitions shall apply in this AUP (unless otherwise specified). The Agreement takes precedence over any conflicting provisions in this AUP. Entrust may modify this AUP at any time. Entrust will take commercially reasonable efforts to provide You with written notice (email or posting notice at the Service portal to suffice as adequate notice). 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).

Thus, You agree not to use, and not to encourage or allow any end user (including without limitation Users) to use, the Service in the following prohibited ways.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others (i) to use the Service for any illegal, harmful, fraudulent, infringing, abusive or offensive use, or for any other activities that materially interfere with the business or activities of Entrust; or (ii) to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include, without limitation:

- **Illegal, Harmful or Fraudulent Activities**. Any activities that: (i) are illegal, that violate the rights of others, or that may be harmful to others, Entrust operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming; (ii) violate or facilitate the violation of any local, state, provincial, federal, or foreign law or regulation, including, but not limited to, laws and regulations regarding the transmission of data or software and recording of phone calls and communications; (iii) use the Service in any manner that materially violates telecommunications industry standards, policies and applicable guidelines published by generally recognized industry associations, including those specifically communicated in writing to You by Entrust; (iv) use the Service to harvest or otherwise collect information about individuals, including email addresses or phone numbers, without their explicit consent or under false pretenses; (v) violate the privacy or data protection rights of any person (e.g. collecting or disclosing any information about an identified or identifiable individual protected under the privacy and/or data protection legislation applicable in the individual's jurisdiction without written permission); constitute cooperation in or facilitation of identity theft; (vi) degrade or negatively influence the good will or reputation of Entrust or that of its affiliates, customers, partners or other third party service providers; or (vii) use the Service in a manner that triggers a law enforcement, government, or regulatory agency to request the suspension of the Service to Customer and/or its related phone numbers.

- **Infringing Content**. Content that infringes or misappropriates the intellectual property or proprietary rights of others.

- **Offensive Content**. Content that: (i) is defamatory, illegal, obscene, offensive, inappropriate,

pornographic, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts; or (ii) is, facilitates, or encourages libelous, defamatory, discriminatory, or otherwise malicious or harmful speech or acts to any person or entity, including but not limited to hate speech, and any other material that Entrust reasonably believes degrades, intimidates, incites violence against, or encourages prejudicial action against anyone based on age, gender, race, ethnicity, national origin, religion, sexual orientation, disability, geographic location or other protected category;

- **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, spyware, worms, time bombs, cancelbots, or any other malicious, harmful, or deleterious programs.

No Security Violations

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

- **Unauthorized Access**. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.

- **Interception**. Monitoring of data or traffic on a System without permission.

- **Falsification of Origin**. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route (including creating a false phone number), or otherwise attempting to mislead others as to the origin of a message or phone call. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

- **Creating False Identity**. Creating a false identity or phone number, or otherwise attempting to mislead others as to the identity of the sender.

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:

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

- **Denial of Service (DoS)**. Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective. Launching or facilitating, whether intentionally or unintentionally, a denial of service attack on the Service or any other conduct that materially and adversely impacts the availability, reliability, or stability of the Service.

- **Computer Viruses**. Do not intentionally distribute a computer virus or in any other way attempt to interfere with the functioning of any computer, communications system, or website, including the computer, and communications systems used to provide the Service. Do not attempt to access or otherwise interfere with the accounts of customers and/or users of the Service or the Service itself;

- **Intentional Interference**. 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.

- **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

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 30 days of receiving consent, then You will need to reconfirm consent (see “Double Opt-in” below).

- The consent applies only to You, and to the specific use or campaign that the recipient has

consented to. You can't 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.

Alternative Consent Requirements: The Two Exceptions

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.

- *Contact initiated by You to send informational content to an individual based on having a prior relationship*

You may send an outbound message that provides information requested by the individual, or that can be reasonably expected by the individual based on Your relationship. An example of such a relationship and message is a dentist reminding a patient of an appointment.

In addition to appointment reminders, other examples include receipts, one-time passwords, order/shipping/reservation confirmations, drivers coordinating pick up locations with riders, and repair persons confirming service call times.

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

The individual must have knowingly provided their phone number to You, and have taken some action to trigger the potential for communication. Actions can include a button press, setting up an alert, making an appointment, or placing an order.

NOTE: The alternative consent requirements cannot be used for promotional content such as marketing, coupons, advertisements, notifications regarding a job opportunity, and sweepstakes, independent of whether the individual initiates contact, or You have consent for informational content of the type noted above based on a prior relationship.

Double Opt-in Consent

We require double opt-in consent in some limited use cases. Many of these use cases listed below generate the majority of complaints about unwanted messages which is why the burden of consent is higher.

- Affiliate marketing including multi-level marketing - this is typically a marketing arrangement which an online retailer pays commission to an external website for traffic or sales generated from its referrals.

- Lead generation services

- Sweepstakes
- Financial products, unless You are the financial institution directly offering the product. These include debt refinancing, short-term credit offers, and payday loans
- Job alerts
- Work-from-home offers

Double opt-in is a two-step process:

- First, the message recipient must knowingly provide consent to You or Your customer prior to receiving any text message. That consent must be provided through an electronic signature or some other online sign-up form that makes clear to the individual they are agreeing to receive messages of this type.
- Second, in Your first text message to that individual, You must identify yourself and prompt the individual to confirm their consent.

For example, Your first outbound message would be compliant if it included text similar to, “This is Company X. You recently signed up to receive text messages from us. Please reply YES to confirm or STOP to unsubscribe.” Only after You receive the confirmation “YES” may You send a follow-up message with information related to a topic listed above.

Identifying Yourself as the Sender

Every message You send must clearly identify You as the sender, except in follow-up messages of an ongoing conversation.

Message Recipient 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 also 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.

Periodic Messages and Ongoing Consent

In some cases, You may want to periodically send messages to an individual who earlier provided proper consent. This practice is allowed, provided that Your message includes a reminder to the individual about how to unsubscribe. If You send more than one message in a given month, You need to include the reminder in just one of those messages--not in all of the messages that You send in that month.

You must respect the message recipient’s preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent no less often than once every 18 months.

Age and Geographic Gating

If You are sending messages in any way related to alcohol, firearms, gambling, tobacco, or other adult content, then more restrictions apply. In addition to obtaining consent from every message recipient, You must ensure that no message recipient is younger than the legal age of consent based on where the recipient is located. You also must ensure that the message content complies with all applicable laws of the jurisdiction in which the message recipient is located. Additionally, this AUP bans sending any content that is offensive, inappropriate, pornographic, obscene, illegal, or otherwise objectionable, even if the content is permissible by law and appropriate age restrictions are in place.

You need to be able to provide proof that You have in place measures to ensure compliance with these restrictions.

Content We Do Not Allow

The key to ensuring that messaging remains a great channel for communication and innovation is preventing abusive use of messaging platforms. That means we never allow some types of content on our platform, even if our customers get consent from recipients for that content. Those content types include:

- Anything that's illegal in the jurisdiction where the message recipient lives. For example, we do not allow messages related to the sale of recreational or medicinal cannabis in the United States, because United States federal laws prohibit its sale.

- Hate speech or harassment, or any communications from groups whose primary purpose is deemed to be spreading hate.

- Fraudulent messages.

- Malicious content, such as malware or viruses.

- Any content that is designed to intentionally evade filters.

How We Handle Violations

When we identify a violation of these principles, we work with You in good faith to get You back into compliance. To protect the continued ability of all our customers to freely use messaging for legitimate purposes, we reserve the right to remove access to the Service (or portions thereof) for customers that we determine are not complying with this AUP, or who are not following the law in any applicable area.

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this AUP or misuse of the Service. We may:

- investigate violations of this AUP or misuse of the Service; or

- 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.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing

network and systems information related to alleged violations of this AUP.

Reporting of Violations of this AUP

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