Workflow Signing Service
Terms of Use

Entrust's Workflow Signing (formerly Signhost) service is subject to these Offering-specific terms of use (the "Workflow Signing Schedule") and the Entrust General Terms and Conditions ("General Terms") available at https://www.entrust.com/general-terms.pdf. 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 HOSTED SERVICES. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICES 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. "Additional Work" means work or other services delivered by Entrust that do not fall under the contents and/or scope of the work described in the Agreement, or changes therein (including amended functional specifications), including any extra work requested by the Customer via the Hosted Service, as well as other extensions/upgrades requested by the Customer.

1.2. "Administration Information" means information in and related to Customer's Online Portal account and information generated by Customer's usage of the Hosted Service, such as Customer's access credentials, contact information for Workflow Signing Administrators, license entitlements, and credit consumption.

1.3. "API Link" means an application programming interface that facilitates automated use of the Workflow Signing Cloud Services from the Customer's systems.

1.4. "Biometric Data" means, collectively, all "biometric identifiers" and "biometric information," as those terms and equivalent terms are defined in applicable Biometric Data Protection Laws.

1.5. "Biometric Data Protection Laws" means, collectively, all applicable laws with respect to the collection, capture, possession, and use of biometric data, including the Illinois Biometric Information Privacy Act (BIPA), Texas Capture or Use of Biometric Identifier Act (CUBI), and Washington Biometric Law.

1.6. "Customer Content" means any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by, or otherwise sent, received or accessible through, the Hosted Service, and any computational results that Customer or any User derives from the foregoing through its use of the Hosted Service, and includes Biometric Data and Administration Information as well as any branding, logos or trademarks provided by Customer or its Users.

1.7. "Hosted Service" means, in this Workflow Signing Schedule, the specific Workflow Signing Cloud Services and the specific elements and services thereof, the Customer's Online Portal account, and the API Link if included in Customer's purchase, that Customer has purchased as specified in the Order.

1.8. "Online Portal" means a cloud-hosted user interface that identifies Customer by its chosen username, tracks Customer's entitlements with respect to the Workflow Signing Cloud Services,

and enables Customer, as applicable in accordance with its entitlements, to administer, configure and use the Workflow Signing Cloud Services.

1.9. "Signer" means any individual invited to apply a digital signature using the Customer's Hosted Service.

1.10. "Workflow Signing Cloud Services" means Entrust's cloud platform providing tools for digital document signature, including access to remote verification/authentication tools.

1.11. "User" has the meaning set out in the General Terms, and in this Workflow Signing Schedule, includes Customer's Affiliates, Workflow Signing Administrators (as defined below), and Signers.

2. **Hosted Service Details**.

2.1. Professional Services. Entrust may provide set-up support and/or other Professional Services for some deployments of the Hosted Service, as specified in an Order, in which case the Professional Services will be provided in accordance with the applicable Order, the General Terms, and, if applicable, a Schedule describing the particular bundle of Professional Services purchased.

2.2. Hosted Services Provision. Following the completion of the set-up of the Hosted Service, Entrust will provide and operate the Hosted Service in accordance with the Documentation and Customer's Order(s) for the Hosted Service. For clarity, the Hosted Service is subject to the operational limitations set out in the Documentation such as maximum number of documents per transaction, file size, numbers of pages, logins, authentications and Signers. For additional clarity, Entrust does not assume any responsibility under this Workflow Signing Schedule for compliance with any digital signature legislation or other external requirements in any jurisdiction.

2.3. Compliance and Security Measures. Entrust will implement and maintain commercially reasonable physical and procedural security controls for the Hosted Services.

2.4. Service Levels. If Customer's Order includes a "Service Level Agreement" service plan, Entrust will provide the service level commitments for the Hosted Service set out at www.entrust.com/workflow-signing-uptime-service-levels.

2.5. Hosted Services Revisions. Entrust may modify Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to the Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice on Entrust's website constitutes written notice). It will be Customer's responsibility to notify its Users of any such changes.

2.6. Customer-requested Modifications. If Customer wishes to have modifications made to the Hosted Services beyond the inherent configurability and flexibility described in the Agreement and applicable Documentation ("Customer-Requested Modifications"), these would require separate written agreement between the parties, including agreement on fees, support, and other responsibilities for such Customer-Requested Modifications. Any Customer-Requested Modifications are outside the scope of this Workflow Signing Schedule.

3. **Grant of Rights**. Customer receives no rights to the Hosted Service other than those specifically granted in this Section 3 (Grant of Rights).

3.1. General. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service, and to grant its Users the ability to access and use the Hosted Service, in each case (a) in accordance with this Workflow Signing

Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order, Documentation, or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Service that Customer is permitted to use, such as limits associated with credits, subscription levels, on numbers or types of identities, verification/authentication tools, Users, signatures or devices, and on types of deployment (e.g. high availability, test or disaster recovery); and (d) subject to the restrictions set out in Section 6 of the General Terms (Customer Responsibilities).

3.2. Evaluation. At Entrust's discretion, it may provide Customer with access to and right to use the Hosted Service for proof of concept, trial, evaluation or other such purposes ("Evaluation Purposes"), for a fee or free of charge, in which case, notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by the parties will apply. The Hosted Services made available for Evaluation Purposes may have a more limited range of functions. The license granted in Section 3.1 (General) shall apply to Hosted Services made available for Evaluation Purposes with the following variations: the term of the license grant is the period specified by Entrust at its discretion, and the use of the Hosted Services will be limited solely to Evaluation Purposes. Entrust may extend the evaluation period in writing at its discretion. Evaluation Purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.1 (Professional Services), 10 (Support), and 14.1 (Term) do not apply to any use of the Hosted Service under the Evaluation Purposes license. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice.

4. **Transactions and Credits.**

4.1. Transactions made using the Hosted Services consume credits purchased by Customer pursuant to an Order (including Orders made via the Online Portal). Customer is responsible for purchasing the quantity of credits that it requires in a timely fashion so that credit inventory is available when needed for transactions. Entrust may provide guidance in Documentation regarding the typical time lapse between purchase and credit inventory appearing in Customer's account. The amount of credits consumed by different types of transactions are as set out in the Documentation or at https://www.entrust.com/legal-compliance/terms-conditions, as updated by Entrust from time to time.

4.2. Customer is responsible for the use of its credits by all its Users, including any accidental consumption of credits due to Users' misconfiguration or incorrect use of the Hosted Services.

4.3. Credits are valid during the Offering Term. Entrust may remove expired credits from Customer's account. Credits cannot be refunded for any reason, including credits that have not been consumed during the Offering Term.

4.4. Entrust will notify Customer if Customer's transactions are at risk of consuming more than the number of purchased credits available in its account. If Customer's consumption exceeds the number of available purchased credits despite this warning, Entrust is entitled to charge the Customer in arears for the excess credits consumed ("Overage Credits"). Fees for Overage Credits are specified in the Order, or, if such information is absent, will be 20% higher than the list price for credits. If the Customer's excess consumption exceeds the available purchased amount of credits by two hundred percent (200%) or more, Entrust is authorized to suspend the Hosted Services and other obligations under the Agreement.

5. **Customer Roles and Responsibilities**.

5.1. Appropriate Use. Customer will decide how it will use the Hosted Services, and for which specific objectives. Customer is responsible for the correct use of the Hosted Services in accordance with the Documentation and in accordance with Customer's own internal and external requirements, including provision of requested inputs by Users. Without limiting the foregoing, Customer is responsible for choosing electronic signature, authentication and electronic identification tools

and methods from those made available through the Hosted Services, all as appropriate for the Customer's purposes, including suitability of use in accordance with laws and regulations applicable to the Customer's business and transactions. Entrust disclaims all responsibility and liability for non-functioning of the Hosted Services as a result of a User's failure to comply with the Documentation.

5.2. Use of API Link Key. If the Hosted Services include the API Link, Customer will receive access and the ability to generate its API Link key via the Online Portal. The Customer must keep the API Link key strictly confidential and only use it for the Customer's own use of the API Link.

5.3. Workflow Signing Administrators. Customer exercises its rights and obligations with respect to the Hosted Services through individuals that the Customer appoints at its discretion ("Workflow Signing Administrators"). The Workflow Signing Administrators initially appointed by Customer will be provided to Entrust during account set-up. Each Workflow Signing Administrator will have the ability to appoint and set permissions for additional Workflow Signing Adminstrators. Workflow Signing Administrators may have the ability to make Orders and changes to the Hosted Services via the Online Portal. Customer agrees that it is responsible for the supervision of its Workflow Signing Administrators and that Entrust is entitled to rely on instructions provided by the Workflow Signing Administrators with respect to the Hosted Service as if such instructions were provided by the Customer itself.

5.4. Customer-hosted Components. If Customer's Order for the Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (collectively, "Customer-hosted Products") Customer will be responsible for the lifecycle management (patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement commercially reasonable security measures with respect to the Customer-hosted Products and the environment where they are installed. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures; and (iii) for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Service. Customer understands if it fails to comply with this Section it could create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust may have the right to suspend the Hosted Service in accordance with Section 13 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

5.5. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Service(s), including facilities to terminate VPN tunnels as specified by Entrust, and any components identified as being on Customer's site or environment in the Documentation. Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

5.6. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Hosted Services, including, without limitation, by securing, protecting and maintaining the confidentiality of its access credentials and any access credentials issued to its Users. Customer is responsible for any access and use of the Hosted Services via Customer's Online Portal account and API Link and for all activity that occurs in Customer's Online Portal account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Services or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

6. **Customer Content**.

6.1. Customer's Responsibility for Compliance. Customer shall be responsible for the accuracy, quality and legality of Customer Content, the means by which Customer acquired it, and Customer's use of Customer Content in and through the Hosted Service. Without limiting the generality of the foregoing, Customer's use of the Hosted Service may involve the collection and processing of Biometric Data. Customer shall, at all times during the Term, comply with the Biometric Data Protection Laws.

6.2. Storage. Customer is responsible for keeping its own copies of Customer Content for storage, backup, evidentiary and other purposes outside of the Hosted Services. Customer Content is only stored in the Hosted Services temporarily, and for no longer than necessary for Entrust's provision of the Hosted Services in accordance with the Agreement. Entrust may impose a maximum limit on the amount of storage space or data traffic that the Customer may use each month in connection with the Hosted Services.

6.3. Biometric Data Notices. Customer shall provide, and shall be solely responsible for providing, a notice to each Signer whose Biometric Data will be collected ("Signer Biometric Notice") that (i) complies with all applicable Biometric Data Protection Laws; (ii) accurately and completely describes the purposes for the collection, use, processing, and storage of such Signer's biometric data by Entrust and Customer, and any permitted or required disclosures of such biometric data by Entrust and Customer, and (iii) does not conflict with Entrust's Biometric Data Notice, available at https://www.entrust.com/legal-compliance/data-privacy or the applicable Entrust Product Privacy Notice. Such Signer Biometric Notice shall be provided prior to obtaining the Signer's consent as set forth in Section 6.4 (Consents) below.

6.4. Consents. Customer shall obtain, and shall be solely responsible for obtaining, all requisite User consents, including any consents from Signers required under applicable Biometric Data Protection Laws with respect to the collection, use, processing, storage, and disclosure of each Signer's Biometric Data in connection with the Hosted Service and for the purposes set forth in Entrust's Biometric Data Policy and the applicable Entrust Product Privacy Notice.

6.5. Notice & Consent Tools. As part of the Hosted Service, Entrust may offer features and functionalities that enable Customer to provide notice to a Signer or obtain a Signer's consent for the collection, use, processing, storage, and disclosure of Biometric Data. Such features and functionalities are for Customer's convenience only, and Entrust does not warrant that those features and functionalities comply, in whole or in part, with applicable Biometric Data Protection Laws, and Entrust shall not be responsible or liable for Customer's use of such features or functionalities in any way. Customer is solely responsible for determining the appropriateness of using the features and functionalities provided by Entrust and assumes all risks associated with such use.

6.6. Biometric Data Retention Policy. To the extent that applicable Biometric Data Protection Laws require Customer to post a publicly available written policy that includes a retention schedule and guidelines for permanently destroying biometric data ("Customer Biometric Data Retention Policy"), such Customer Biometric Data Retention Policy shall not conflict with Entrust's Biometric Data Policy or the applicable Entrust Product Privacy Notice.

6.7. Authorization. Customer hereby grants Entrust (including any of its applicable Affiliates, subcontractors or hosting service providers): (a) all rights and consents required for the collection, use, and disclosure of the Customer Content in accordance with the Agreement; and (b) a non-exclusive, nontransferable worldwide right to copy, store, record, transmit, display, view, print or otherwise use any trademarks that Customer uploads into the Hosted Service for the purpose of applying Customer's branding to portions of the Hosted Service. Customer represents and warrants that Customer (and/or Users) has or will have sufficient rights to enable Customer and its Users to transfer the Customer Content to Entrust and grant Entrust the rights set out above.

6.8. Documentation. Upon Entrust's request, Customer will promptly provide information and

documentation sufficient to substantiate Customer's compliance with this Section 6 (Customer Content), including, for example, the content of the Signer Biometric Notice Customer provides to Signers and records documenting the consents that have been obtained from Signers.

6.9. Customer Content and Administration Information. Entrust agrees to access and use the Customer Content only to the extent necessary to provide the Hosted Service, or as necessary to comply with law or a binding order of a government body. Notwithstanding the forgoing, Administration Information may be processed for the purposes of billing, providing Support and to investigate fraud, abuse or violations of this Agreement in the United States, Canada and other locations where Entrust maintains its support and investigation personnel.

6.10. Cloud Risks. Customer understands that the Hosted Service is a cloud-hosted service. Although Customer Content may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Hosted Services except as expressly provided in this Workflow Signing Schedule, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Customer Content or any data stored in, transferred to or from, or otherwise processed by the Hosted Service, including in transit.

6.11. Non-Disclosure. For the purposes of this Workflow Signing Schedule, the definition of "Confidential Information" in the General Terms excludes any Customer Content. Except as otherwise provided in this Section (Customer Content) or in the Agreement, Entrust shall not disclose to any third party any Customer Content that Entrust obtains in its provision of the Hosted Service. However, Entrust may make such information available (i) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Entrust's legal counsel, (ii) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by Customer in the opinion of Entrust and (iii) to third parties as may be necessary for Entrust to perform its responsibilities under this Agreement. In addition, to the extent required by applicable law, Entrust may provide Customer's contact information and relevant Customer Content to a Signer in response to a complaint that Customer's use of the Hosted Services has breached the Signer's rights or this Agreement, provided that the complaint is reasonably plausible and the information is not otherwise readily available to the Signer.

7. **Software.** If Entrust provides any Software in connection with the Hosted Service, the Schedule provided with the Software will apply (and not this Workflow Signing Schedule, with the exception of Section 4.2 (On-premise Components)). If no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license available at https://www.entrust.com/end-user-license.pdf.

8. **Public Trust Services.** If Entrust provides any public trust services or certificates in connection with the Hosted Service, the terms and conditions applicable to such services and certificates are those provided in the Entrust repository at https://www.entrust.net/cps.

9. **Open Source Software and Third Party Products.**

9.1. 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 Offering ("Ancillary Software"). If a separate license agreement pertaining to Ancillary Software is embedded or provided with the Offerings, then the Ancillary Software is subject to the applicable separate license agreement pertaining to the Ancillary Software. Upon request, Entrust will provide Customer with a complete list of Ancillary Software and corresponding licenses, which list shall be deemed Entrust Confidential Information.

9.2. Third Party Products and Services. Certain third-party hardware, software and services, such as

identity verification or authentication services, may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("Third Party Vendor Products"). Except as expressly stated in this Workflow Signing 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 applicable third party vendor's terms, conditions and policy documents ("Vendor Terms") provided to Customer, set out below, accompanying, embedded in, or delivered with the Third Party Vendor Products, or otherwise made available by the third party vendor. In particular:

9.2.1. If Customer uses the verification method 'iDIN', Customer agrees that it will comply with the 'iDIN Additional Terms', available at www.entrust.com/workflow-signing-idin-terms.

9.2.2. If Customer uses the verification method 'itsme', Customer agrees that it will comply the 'itsme Additional Terms' available at www.entrust.com/workflow-signing-itsme-terms.

9.3. No Standalone Use. Any Third Party Vendor Product or Ancillary Software included with or embedded in the Offering may be used only with the applicable Offering, unless otherwise permitted in the applicable agreement accompanying such Third Party Vendor Product or Ancillary Software.

9.4. Availability not guaranteed. Entrust has no obligation to maintain or continue providing access to Third Party Vendor Products through or in connection with the Hosted Services, including with any verification suppliers, and may discontinue such access at any time at its sole discretion.

10. **Support.** Entrust provides the support commitments set out in the Support Schedule available at www.entrust.com/workflow-signing-support-schedule for the Hosted Services and any Software provided in connection with the Hosted Services. The "Basic Service Plan", as described in the Support Schedule, is included at no additional charge with a subscription to a Hosted Service. Other levels of Support may be available for purchase for an additional fee.

11. **Interoperability.** Third parties may make available plugins, agents, or other tools that enable the Hosted Service to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Service, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Service with such Interoperation Tools under this Workflow Signing Schedule. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Service, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

12. **Indemnification**. In addition to the indemnification obligations in the General Terms, Customer shall defend, indemnify and hold harmless Entrust, its Affiliates and licensors, and each of their respective officers, directors, employees, and representatives, against any and all claims, actions, demands, suits, hearings, proceedings, judgments, fines, penalties, costs, losses, damages, liabilities, settlement fees, and expenses (including investigation costs and attorney's fees and disbursements), arising out of or relating to any of the following: (i) Customer's breach of Section 6 (Customer Content); (ii) Customer's breach of the terms and conditions referenced in Section 9 (Open Source Software and Third Party Products); (iii) a violation of applicable law by Customer, Users, or Customer Content; (iv) an allegation that the Customer Content infringes or misappropriates a third party's intellectual property rights; and (v) a dispute between Customer and any User (each of (i)-(v) are deemed included in the definition of "Customer Indemnified Claim" in the General Terms). NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE IN THE AGREEMENT, CUSTOMER'S LIABILITY WITH RESPECT TO THE INDEMNITY IN PARAGRAPH (i) OF THIS SECTION 12 (INDEMNIFICATION) WILL NOT BE SUBJECT TO ANY LIMITATION OR EXCLUSION.

13. **Fees.** Customer will pay the costs and fees for the Hosted Services, including the fees for the credits to be used against certain aspects of the Hosted Services, as set out in the applicable Order, which are payable in accordance with the Order, this Schedule and the General Terms. If the information provided by the Customer at the time of the acceptance of the Order proves to be incorrect, such as the quantity of credits required for Customer's usage, Entrust has the right to adjust the Customer's credits and entitlements accordingly, including adjusting the fees payable and the package composition. Entrust will notify Customer of any such adjustments.

14. **Term & Termination**.

    14.1. Term. The Hosted Services are sold on a subscription basis for the Offering Term set out in the applicable Order. All subscriptions are non-cancellable and non-refundable.

    14.2. Termination. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement for the Hosted Services (i) if Customer commits a material breach of this Workflow Signing Schedule and fails to remedy such material breach within 30 days (or such longer period as Entrust may approve in writing) after delivery of the breach notice; (ii) if Customer has not logged in and/or used the Hosted Services for a period of twelve months and fails to respond within 30 days to an email notification of deactivation sent to the email address on Customer's account; and (iii) for any reason by providing Customer advance notice of at least 1 year, unless Entrust discontinues the general commercial availability of the Hosted Service, in which case Entrust may terminate the Agreement upon 180 days' notice to Customer.

    14.3. Effects of Termination or Expiry. Upon expiration of the Offering Term (unless succeeded immediately by a renewal Offering Term) or termination of the Agreement for a Hosted Service: (i) Customer must immediately cease all use of the Hosted Service; and (ii) Entrust may revoke access to the Hosted Service and delete or render inaccessible all Customer Content.

15. **Suspension**. In the event that Entrust suspects any breach of the Agreement by Customer and/or Users, Entrust may suspend Customer's, and/or such Users' access to and use of the Hosted Service without advanced notice, in addition to such other remedies as Entrust may have pursuant to the Agreement. Nothing in the Agreement requires that Entrust take any action against any Customer, User or other third party for violating the Agreement, but Entrust is free to take any such action at its sole discretion.