Last updated July 11, 2017

IntelliTrust Acceptable Use Policy

1. Acceptable Use

All customers and users of the IntelliTrust[tm] cloud-based authentication platform (the "**Service**") are required to conduct themselves with respect for others. While not exhaustive, the following rules must be observed during use of the Service. By using the Service, you agree to the latest version of this Policy. If you violate the Policy or authorize or help others to do so, we may suspend or terminate your use of the Services.

1. Do not violate the privacy rights of any person. Do not collect or disclose 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. Do not cooperate in or facilitate identity theft;

2. Do not access any computer or communications system without authorization, including the computers used to provide the Service. Do not attempt to penetrate or disable any security system. Do not intentionally distribute a computer virus, launch a denial of service attack, 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;

3. Do not violate any laws applicable in the country of use;

4. Do not use the Service in any way which may degrade or negatively influence the good will or reputation of Entrust Datacard Limited, Entrust Inc. or their respective affiliates (collectively "**Entrust Datacard**"), customers, partners or any other third party; and

5. Do not use the Service in any morally distasteful way.

2. Reporting and Co-operation

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services. 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, user, authentication, and/or other 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 same related to alleged violations of this Policy.

3. Revision of AUP

Entrust Datacard may change this AUP at any time. Entrust Datacard will take commercially reasonable efforts to provide you with written notice (email or posting notice at the Service portal to suffice as adequate notice).

4. Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation.