PoolPass Acceptable Use Policy

This Acceptable Use Policy (this "Policy") describes prohibited uses of the PoolPass cloud service (the "Service") and the website located at http://www.pool-pass.com (the "Website"). The examples described in this Policy are not exhaustive. We may modify this Policy at any time by posting a revised version on the Website. By using the Service or accessing the Website, 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 Service.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others to use, the Service or Website for any illegal, harmful, fraudulent, infringing, or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing, or offensive. Prohibited activities or content include:

1. Illegal, Harmful or Fraudulent Activities. Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation.
2. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
3. Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.

No Security Violations

You may not violate the security or integrity of the Service or Website or its communication system, software, or computing devices. Prohibited activities include:

1. Unauthorized Access. (a) Accessing or using the Service without permission, including attempting to probe, scan, or test the vulnerability of the Service or to breach any security or

authentication measures used by the Service; (b) Accessing content stored on the Service that does not belong to your account, including our data or our clients' or customers' data; (c) Attempting to use the Service outside of the supplied PoolPass software (the "Software").
2. Interception. Monitoring of data or traffic on the Service or Website without permission.
3. Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route.
4. Avoiding Restrictions. Using manual or electronic means to avoid any limitations or bypass any license restrictions placed on the use of the Service or Software, such as access and storage restrictions.

No Network Abuse

1. You may not make network connections to the Service without an authorized account.
2. You may not disrupt the Service or Website through monitoring, probing, Denial of Service (DoS), or otherwise interfere with the proper functioning of the Service or Website, including any deliberate attempt to overload the Service or Website by mail bombing, broadcast attacks, or flooding techniques.

Our Monitoring and Enforcement

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

1. Remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Service.
2. 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 Policy.

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.

This policy was updated February 10, 2018