RECENT UPDATES

This Attachment to the Cloud Service Agreement has been revised as part of our 2017 policy updates. Please review in its entirety. Changes include but are not limited to:

- Sections 14 and 15 updated to specify Customer's non-usage of testing tools within the Cloud environment.
- Section 16 added to disallow the use of anonymised or misleading networking end points.
- Section 17 onward renumbered. update notes

Cloud Service Agreement Attachment 2: Acceptable Use Policy (2017-06-02)

This Acceptable Use Policy (AUP) is only to be construed alongside the Cloud Service Agreement (CSA). It forms part of the CSA as per Section 1 of that document and runs concurrently with it.

This AUP specifically describes how the Customer should (and should not) use the service. If Customer breaches the AUP, the Customer is at fault.

This AUP supplements other related Sections in ASPL policies, especially but not limited to Section 9 (Use of Our Products and Services) in the Terms and Conditions, Section 7 (Rights and Limitations) in the EULA and Section 4 (Cloud Data) of the Privacy Policy.

In accordance with Section 5 (Obligations of the Customer) of the CSA, the Customer shall comply with the following terms of use of the Services:

While using the Services, the Customer SHALL NOT:

1) infringe any Third Party's Intellectual Property Rights;

2) infringe ASPL's Intellectual Property Rights;

3) breach any applicable law, regulations or order of the authorities;

4) process Third Party's Personal Data illegally;

5) breach any other Third Party's rights which are different from above points 1) and 4);

6) upload or introduce malicious code, viruses, trojan horses, e-mail bombs, spyware, malware or other similar software;

7) allow Third Parties external to the Customer's organisation to use the Services unless authorised in writing by ASPL;

8) send unsolicited e-mail or communications of any kind;

9) support in any way illegal activities;

10) misrepresent or obscure the identity of the Customer's users;

11) upload illegal Contents on the System;

12) violate any applicable export and re-export control legislation or regulations;

13) upload or introduce encryption software in violation of national or international exporting legislation;

14) use means which can cause a breach of security of ASPL's service or equipment, including Penetration Testing, Performance Testing or executing Monitoring Agents against the service;

15) use means which can cause a disruption of the Services, including Penetration Testing, Performance Testing or executing Monitoring Agents against the service;

16) use anonymised or misleading networking end points.

While using the Services, the Customer SHALL:

17) adopt secure usernames, passwords and any other security measures in relation to the access to the System in line with best practice and any instructions provided by ASPL;

18) inform ASPL in case of loss of any usernames, passwords or any other security measures for accessing the Services, not later than 3 (three) Working Days from the discovery;

19) inform all the Customer's Users (employees, officers, consultants) of the terms and conditions of the AUP;

20) process Personal Data of Third Parties in accordance with applicable legislation (e.g. if so required under applicable law, provide full notice to the Data Subjects and obtain their valid consent, notify the Processing of Personal Data with the competent data protection authority, implement any security measures on its side of the Service to ensure full compliance with the legislation, monitor the Services);

21) obtain the consent of the owners of the Intellectual Property Rights to use their works on or through the Services.