RIB Cloud Services - Acceptable Use Policy

This Acceptable Use Policy ("AUP"), along with the separate agreement with us (the "RIB General Terms and Conditions"), describes the acceptable use of and access to the cloud Services offered by RIB. By using the cloud Services, you (“Customer”) agree to be bound by this AUP in addition to the terms of the RIB General Terms and Conditions. **If Customer violates this AUP or authorizes or helps others to do so, RIB may (in addition to any other rights or remedies that RIB may have under the RIB** General Terms and Conditions **or otherwise) suspend or terminate Customer’s use of the cloud Services in accordance with the terms of the RIB** General Terms and Conditions. Any terms not defined herein shall have the meanings ascribed to them in the RIB General Terms and Conditions.

Prohibited Activities

Customer may not upload Customer Data or use the Services in a manner that RIB believes:

1. Violates any local, state, national, foreign, or international statute, regulation, rule, order, treaty, or other law (each a "Law"), including, but not limited to, the Digital Millennium Copyright Act, or those Laws concerning child pornography and illegal gambling;
2. Is abusive, deceptive, pornographic, obscene, defamatory, slanderous, offensive, or otherwise inappropriate;
3. Violates or otherwise encroaches on the rights of others, including, but not limited to, infringing or misappropriating any intellectual property or proprietary right of another;
4. Advocates or induces illegal activity;
5. Stalks, harasses, or harms anyone, including minors;
6. Impersonates any person or entity or otherwise misrepresents Customer's affiliation with a person or entity;
7. Modifies, alters, tampers with, repairs, or otherwise creates derivative works of any software included in the Services;
8. Except as allowed by local law, reverse engineers, disassembles, or decompiles the Services or software included in the Services;
9. Accesses or uses the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
10. Interferes with or disrupts the Services or servers or networks connected to the Services;
11. Uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Services or any other accounts, computer systems, or networks connected to the Services (each a "System"); Where Customer is permitted to access the Cloud Services by any RIB-provided Application Programming Interface (“API”), Customer will ensure that usage does not exceed any volume limits specified by RIB.
12. Attempts to gain unauthorized access to any portion of the Services or any System, whether through hacking, password mining, or any other means;
13. Violates the security or integrity of a System, including, but not limited to:
    - Accessing or using any System without permission, including attempts to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System;
    - Monitoring data or traffic on a System without permission;

- Forging packet or email headers, or any part of a message describing its origin or route;
- Uploading Customer Data that contains viruses, worms, corrupt files, Trojan horses, or other forms of corruptive code, or any other content that may compromise the Services; or
- Hacking, destabilizing, or adapting the Services, or altering another website to falsely imply it is affiliated with the Services;

14. Connects to any users, hosts, or networks where Customer does not have permission to communicate with such users, hosts, or networks, including, but not limited to:

    - Monitoring or crawling a System so that such System is impaired or disrupted;
    - Conducting denial of service attacks;
    - Intentionally interfering with the proper functioning of any System, including any deliberate attempt to overload a System by any means;
    - Operating network services like open proxies, open mail relays, or open recursive domain name servers; or
    - Using means (manual or electronic) to avoid any use limitations placed on a System, such as access and storage restrictions;

15. Distributes, publishes, sends, or facilitates unsolicited mass e-mailings, promotions, advertising, or solicitations, including commercial advertising and informational announcements;

16. Alters or obscures mail headers or assume a sender's identity without the sender's explicit permission; or

17. Collects replies to messages if those messages violate this AUP.

RIB has the sole discretion to determine whether Customer Data or Customer's use of the Services is prohibited. All Customer Data that is provided to RIB or actions that are performed via Customer's account, whether provided or performed by Customer's employees, Customer's contractors, or Customer's other End Users, are the sole responsibility of Customer.

Monitoring and Enforcement

While not obligated to perform investigations, RIB may:

1. Investigate violations of this AUP or misuse of the Services;

2. Investigate and help prevent security threats, fraud, or other illegal, malicious, or inappropriate activity;

3. Remove, disable access to, or modify any Customer Data or resource that RIB believes violates this AUP or any other agreement RIB has with Customer for use of the Services; or

4. Suspend or terminate provision of Services to Customer for uses that violate this AUP or any other agreement RIB has with Customer for use of the Services.

RIB may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. RIB’s reporting may include disclosing appropriate Customer information and/or Customer Data. RIB 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.

Modifications

RIB reserves the right to modify this AUP at any time without notice.

Reporting

Customer is required to immediately report to RIB (i) any event or issue which could compromise the stability, service or security of the RIB network and (ii) any known violation of this AUP.