REDWOOD'S ACCEPTABLE USE POLICY

Purpose and Scope

This Acceptable Use Policy ("**AUP**") is incorporated by reference into, and governed by the Software-as-a-Service ("**SaaS**") agreement and/or related order form between Redwood and Client. This AUP applies to all Clients who have access to and/or use a Redwood SaaS solution and sets forth the acceptable and prohibited use of the SaaS solution by Clients. Client agrees to comply with this AUP and is responsible for adherence to this AUP by all of its affiliates, employees and/or users. Redwood reserves the right in its sole discretion to amend the AUP and publish updated versions at https://www.redwood.com/acceptable-use-policy/. Any terms not defined herein shall have the meanings ascribed to them in the SaaS agreement and/or related order form between Redwood and Client.

Acceptable Use

Client may use the Redwood SaaS solution during the applicable term for Client's internal business purposes only, and in accordance with the SaaS agreement and/or related order form governing the terms and conditions of the SaaS solution between Redwood and Client.

Violations

Client will be in violation of this AUP if Client's use of the SaaS solution causes harm to the SaaS as made available by Redwood or if Client encourages or instructs any third party to violate this AUP. Client may not upload data to the cloud and/or use the SaaS solution in any way that is harmful, illegal, unlawful or offensive to or interferes with the use of the SaaS servers or network, or the network of any other provider, interferes with the use of the SaaS solution received by other clients, infringes or misappropriates with intellectual property rights of others, results in the publication of threatening or offensive material, or constitutes a security risk. The following activities, but not limited to, are prohibited under this AUP:

Related to client activities and client data/content

a) Any illegal activities, including engagement in or promoting or otherwise making available gambling sites, or run gambling operations, or advertising or facilitating child pornography.
b) Any harmful or fraudulent activities that may be harmful to others or Redwood's reputation, including the offering or disseminating fraudulent goods, services, schemes or promotions, such as pyramid schemes, pharming, make-money-fast schemes or phishing, or participate in any other deceptive forward multi-level marketing.
c) Submit, share, store, copy, backup or distribute any illegal files or data that contains a third party's intellectual property right, which may result in an infringement or misappropriation of this intellectual property right.
d) Submit, share, store, copy, backup or distribute any illegal files or data that is obscene, threatening, defamatory, abusive, or otherwise unlawful or tortious material, including data that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.
e) Submit, share, store, copy, backup or distribute any illegal files or data that contains viruses, worms, time bombs, Trojan horses and any other harmful or malicious code, scripts, agents, files or any other similar software that may damage the operation of the SaaS.

Related to security violations

f) Any attempts to hack, gain access to, breach, circumvent, probe, scan or test the vulnerability of the user authentication or security of any host, network, server or user account, including but not limited to, accessing data not intended for Client, logging into or using a server or account without express authorization of Redwood.

g) Monitoring of data or traffic when using the SaaS solution without Redwood's express authorization.
h) Falsification of origin by forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin of route.

Related to network, e-mail and/or system abuse

i) Access or use the SaaS solution in a way intended to avoid fees or exceeding usage limits or using any other means to avoid any other use limitations placed on the SaaS solution, such as access and e-mail restrictions.
j) Engage in activity that interferes with or disrupts the SaaS solution or servers and/or networks connected to the SaaS solution.
k) Use the SaaS solution in a way that results in excessive bandwidth usage, which may have a negative impact on other users.
l) Monitoring or crawling of a system that impairs or disrupts the system being monitored or crawled.
m) Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective (Denial of Service).
n) Use the SaaS solution to send, publish, distribute unsolicited advertising and/or promotional materials, including, without limitation, 'spam' or bulk e-mail

Related to storage restrictions

o) Exceeding the storage restrictions as agreed between Client and Redwood in the SaaS agreement and/or related order form.

In addition to the above, Redwood's SaaS solution may not be used by Client in connection with any criminal, civil or administrative violation of any applicable local, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Consequences of violations of this AUP

Any violation of this AUP by Client will be considered as a material breach of the SaaS agreement and/or related order form governing the terms and conditions of the SaaS solution between Redwood and Client. Upon violation of this AUP by Client, Redwood reserves the right at its sole discretion to apply its statutory and contractual legal remedies (e.g. suspension of Client's access to the SaaS solution and/or termination).

In addition, Redwood reserves the right to investigate any potential violation of this AUP or misuse of the SaaS solution. Amongst others, Redwood may perform the following:

1. Remove, disable access to, or modify any data or content that violates this AUP or the SaaS agreement and/or related order form in place with the Client.
2. Report any activity that potentially violates any law or regulation to appropriate law enforcement officials, regulators, or other third parties. This may include disclosing appropriate client information where necessary.

Last update: 20 February 2019.