Sigil Acceptable Use Policy

Last Updated January 26, 2016

THIS ACCEPTABLE USE POLICY CONTAINS LEGALLY BINDING TERMS APPLICABLE TO YOUR USE OF THE SIGIL SOLUTION AND SERVICES, AS DEFINED HEREIN. IF YOU DO NOT AGREE TO THESE TERMS, YOU MAY NOT USE THE SIGIL SOLUTION OR SERVICES.

Terms of Service/Acceptable Use Policy

1. GENERAL. This Acceptable Use Policy ("Sigil AUP"), including without limitation the following list of prohibited uses described in Section 5 hereof ("Prohibited Uses"), governs the use of the software, hosting services, cloud services and other offerings (the "Offerings") made available by Sigil Technologies Inc. and/or its suppliers, affiliated companies and subsidiaries ("Sigil"). This Sigil AUP is an integral part of your agreement with Sigil and incorporated by reference into the terms pursuant to which we provide you the right to access and use our Offerings. The purpose of this Sigil AUP is to delineate the type of actions and content that are contrary to our mission and philosophies as well as to ensure that your use of our Offerings is in compliance with applicable laws, rules and regulations.

2. USER CONDUCT. This Sigil AUP is intended to protect the Offerings, employees and customers of Sigil, and any end-users from improper, inappropriate, abusive or illegal activity. The prohibited uses described in Section 4 below are intended as general guidelines regarding improper and inappropriate conduct, and should not be interpreted as an exhaustive list.

3. USAGE DATA. Sigil may monitor, collect and use data pertaining to the use of the Solution and Services, provided that any such data collected will be anonymous without reference to the particular Customer, user or end-user. Sigil may only use any such data for its internal research and development purposes and may only publicly disclose such data in an aggregated format that in no way identifies Customer or any particular User (e.g. Sigil may disclose aggregate Page Views statistics for all of its hosted customers).

4. PROHIBITED USES.

4.1 The Offerings may not be used for any of the following purposes:
a) Transmission, distribution, retrieval or storage of any data or other material in violation of any applicable law or regulation.

This prohibition includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

b) Sending Unsolicited Bulk Email (“UBE” or “spam”). The sending of any form of UBE through the Solution or Services advertising a web site, landing page, email address or utilizing any Sigil resources, is prohibited.

c) Solicitation of a customer from, or to collect replies to messages sent from, another Internet Service Provider where those messages violate this Sigil AUP or terms of service of any such provider.

d) Running Unconfirmed Mailing Lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by Sigil customers must be closed-loop (“Confirmed Opt-in”). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list.

4.2 The Offerings may not be used to violate system or network security; such behavior may result in criminal or civil liability. You may not engage, without limitation, in the following activities:

a) Gaining unauthorized access to, or attempting to compromise the normal functioning, operation or security of any network, system, computing facility, equipment, data or information.

b) Engaging in any activities or behavior that may interfere with the ability of others to access or use the Solution, Services or the Internet or that is likely to result in retaliation against the Sigil Solution or Services, Sigil’s employees, officers or other agents, including anything that results in any server being the target of a denial of service attack.

c) Monitoring any data, information or communications on any network or system not owned by you without authorization.
d) Gaining unauthorized access to the user accounts or passwords of other users of any system or network.
e) Attempting to intercept, redirect or otherwise interfere with communications intended for others.
f) Intentionally transmitting files or messages containing computer viruses or propagating worms, Trojan horses, or "spyware"

programs.
g) Uploading and storing information protected under the privacy or security regulations issued pursuant to the Health

Insurance Portability and Accountability Act of 1996 or subject to the Health Information Technology for Economic and Clinical Health

Act.
h) Uploading drivers license numbers, passport numbers, social security, tax ID or similar numbers, bank, checking, credit card,

debit card, financial, or other personal account numbers, and financial or health information.
i) Unauthorized attempts to gain access to an account or computer not belonging to you, or purposely altering or forging your

identity to gain such access. Sending any message or transmitting any electronic communication using a name or address other than your own for purposes of deception is prohibited. Impersonating someone else by altering your source IP address or by using forged headers or other identity information is prohibited. Fraudulently concealing, forging or otherwise falsifying your identity in connection with any use of the Solution or Services.

j) Load testing, probing, scanning, penetration or vulnerability testing of the Services or environment, including without limitation the Hosting Services, to test scalability.

k) Collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting).

5. Customer Responsibilities. You are responsible for the activities of your end-users and you will ensure that your agents or representatives and end-users abide by this Policy. To the extent legally permissible, complaints about your agents, representatives, and end-users will be forwarded to Customer's administrator for action. If violations of the Policy occur, we reserves the right to suspend the Offering or take action to stop the offending action from violating Sigil's Policy as Sigil deems appropriate.

6. Cooperation with Investigations. Our policy is that we will not disclose your data to any third party without your express written consent unless we are required to do so under applicable laws. Nevertheless, Sigil will cooperate with appropriate law enforcement and other governmental agencies and other parties involved in investigating claims of illegal or inappropriate activity, and shall have no liability to you or any third party for any actions taken in connection with such cooperation. You must assist us in these matters when requested.

7. Notification of Violation. If you become aware of any violation of this Sigil AUP by any person, including end-users or third parties, you must immediately notify Sigil via e-mail at contact@sigil.tech, or through your designated Account Manager at Sigil.

8. Contact Us
If you have questions or concerns related to this Acceptable Use Policy please contact Sigil as follows:

Attn: General Counsel

Sigil Technologies Inc.
10707 Ayrshire Dr, Tampa FL 33626.

Or email: contact@sigil.tech