Acceptable Use Policy

September 26, 2018

This Acceptable Use Policy ("AUP") describes the proper use of the services contracted for by a Smarsh client ("Client") under a separate Order Form or Agreement for services referencing this AUP ("Agreement" and the services purchased thereunder "Services"). This AUP is incorporated by reference into the Agreement.

Smarsh may suspend or terminate Client's use of the Services, or the Agreement, if Client or any of Client's users violate this AUP. Client is solely responsible for the data, content, messages, or other information that Client transmits, archives, distributes, displays, uploads or downloads via the Services.

Prohibited Activities

Client shall not use the Services in a manner that:

(a) constitutes or encourages a criminal offense, violates the rights of any person or entity, or violates any local, state, national, or international law, and any rules or regulations promulgated thereunder;
(b) is unlawful, libelous, defamatory, obscene, pornographic, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable, harmful or offensive to third parties;
(c) impersonates any person or entity or otherwise misrepresents any affiliation with a person or entity;
(d) infringes any copyright, trademark, patent, trade secret, or other intellectual property or proprietary right of any person or entity;
(e) is fraudulent or advertises or disseminates fraudulent goods, services, schemes, or promotions (i.e., make money fast schemes, chain letters, pyramid schemes);
(f) is harmful or potentially harmful, including transmitting viruses, Trojan horses, worms, time bombs or any other computer programming routines that could damage, interfere with, surreptitiously intercept, or expropriate any system, program, data or personal information;
(g) covertly gathers information about a user, or covertly transmits information about a user;
(h) could subject Smarsh or any third party to any liability, damages, or danger; or,
(i) violates industry standards or third party agreements or policies.

Client shall not (a) reverse engineer any Service; (b) attempt to bypass or break any security mechanism on any of the Services or use the Services in a manner that poses a security or service risk to Smarsh or other users; (c) use the Services to harvest information or data; (d) create a false identity or forged email address or header, or phone number, or otherwise attempt to mislead others as to the identity of the sender or the origin of a message or phone call.

Laws Specific to Communications

Clients shall comply with all laws that apply to communications, including wiretapping laws, the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, CAN-SPAM Act of 2003 and any other laws or regulations applicable to communications. Client shall not use the Services in a manner that violates: industry standards; any third party policies including all of the applicable guidelines published by the CTIA, the Mobile Marketing Association, or by any other accepted industry associations or carrier guidelines (or any similar or analogous industry standards, third party policies or requirements in any other jurisdiction.

Client's bulk and commercial email practices must meet the following requirements and Client shall, in accordance with applicable law:

(a) obtain consent from e-mail recipients via some affirmative means;
(b) obtain necessary consents in accordance with applicable law;

(c) retain evidence of consents in a form that may be produced on request;
(d) allow a recipient to revoke consent;
(e) post an email address for complaints in a conspicuous place;
(f) have a privacy policy posted for each domain associated with the mailing;
(g) have the means to track anonymous complaints;
(h) not obscure the source of the Client e-mail in any manner; and,
(i) not attempt to send any message to an email address after a certain number of rejections, as required under applicable law.

Interference with Services is Prohibited

Client shall not engage in conduct that has a negative effect on Smarsh or its systems or networks, including overloading servers on the Smarsh network, or taking actions that impose an unreasonable administrative burden on Smarsh.

Client shall not access any part of the Services that Client is not authorized to access or attempt to interfere with the Services. Specifically, Client shall not engage in, or attempt to engage in:

(a) unauthorized access to or use of the Services, data, or the networks or systems, including an attempt to probe, scan or overload a Smarsh system or the Services, or to breach security or authentication measures without express authorization;
(b) unauthorized monitoring of data or traffic on a system without express authorization;
(c) deliberate attempts to overload a system and broadcast attacks;
(d) an action that imposes an unreasonable or disproportionately large load on Smarsh's infrastructure;
(e) performance of a program/script/command or sending messages of any kind that are designed to interfere with a user's terminal session, by any means, including locally or by the Internet;
(f) the use of manual or electronic means to avoid any use limitations placed on the Services, such as timing out;
(g) an attempt to decompile, disassemble, decrypt, extract, reverse engineer or otherwise attempt to derive the source code (including the methods, processes, and infrastructure) underlying the Services or any other software in connection with the Services; or,
(h) any other activity that could be reasonably interpreted as unauthorized access to or interference with the Services.

Updates

Smarsh may revise and update this AUP from time to time.

Current Version of AUP: Version 4, Effective September 26, 2018.