SMARSH ACCEPTABLE USE POLICY

Smarsh provides email hosting services, email encryption and message/content archiving services. This Acceptable Use Policy ("AUP") describes the proper use of the services contracted for by a Smarsh client ("Client") under separate Order Form or Agreement for services referencing this AUP ("Agreement" and the services purchased thereunder "Services"). 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 which Client archives, transmits, distributes, displays, uploads or downloads via the Services.

Prohibited Actions Related to Use of Services

Client is prohibited from using the Services to transmit or store any data, content, messages or other information, in a manner which:

- constitutes or encourage a criminal offense, violates the rights of any person or entity, violates any local, state, national, or international law, or any rules or regulations promulgated thereunder;
- 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;
- impersonates any person or entity or otherwise misrepresent your affiliation with a person or entity;
- infringes any patent, trademark, trade secret, copyright, or other intellectual or proprietary right of any person or entity;
- is fraudulent or advertises or disseminates fraudulent goods, services, schemes, or promotions (i.e., make money fast schemes, chain letters, pyramid schemes);
- is harmful including, without limitation, viruses, Trojan horses, worms, time bombs or any other computer programming routines that may damage, interfere with, surreptitiously intercept or expropriate any system, program, data or personal information; or
- distributes software that covertly gathers information about a user, or covertly transmits information about a user.

Messaging Requirements

Clients of Smarsh Email Hosting are required to comply CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial email using Smarsh hosted email Services or archiving Services. In addition, Client's bulk and commercial email must meet the following requirements and Client must, in accordance with applicable law:

- obtain consent from e-mail recipients via some affirmative means;
- obtain necessary consents in accordance with applicable laws;
- retain evidence of consents in a form that may be produced on request;

- allow a recipient to revoke consent;
- post an email address for complaints in a conspicuous place;
- have a privacy policy posted for each domain associated with the mailing;
- have the means to track anonymous complaints;
- not obscure the source of the Client e-mail in any manner; and
- not attempt to send any message to an email address after a certain number of rejections, as required under applicable law.

Clients who use the Services to communicate and share or receive personally identifiable information are required to comply with all applicable privacy or data protection laws or regulations. Client is responsible for ensuring that:

- the messaging service provider Client uses provides administrative, technological and physical controls required to comply with applicable laws;
- Client complies with applicable laws, industry best practices, and its own corporate policies when transmitting sensitive information (including ensuring that sensitive documents or sensitive information is encrypted or locked);
- Client obtains all necessary consents from the individuals it collects personally identifiable information from, and that Client accurately communicates how it collects, stores, processes and uses personally identifiable information and when Client may share that personally identifiable information with third parties and for what purposes;
- Client maintains a privacy policy that accurately reflects its privacy practices.

Interference with Services Prohibited

Client may not engage in any conduct that has a negative effect on Smarsh or its systems or networks, including, without limitation, overloading servers on the Smarsh network, generating unresolved third-party complaints or complaints which, in the discretion of Smarsh, impose an unreasonable administrative burden on Smarsh.

Client may not access any portion of the Services for which Client is not authorized, or attempt to interfere with the Services in any manner. Specifically, Client may not, without limitation, engage in, or attempt to engage in, any of the following:

- unauthorized access to, or use of the Services, data, or the networks or systems, including any attempt to probe, scan or overload a Smarsh system or the Services, or to breach security or authentication measures without express authorization;
- unauthorized monitoring of data or traffic on any system without express authorization;
- deliberate attempts to overload a system and broadcast attacks;
- any action that imposes an unreasonable or disproportionately large load on Smarsh's infrastructure;

- any program/script/command, or sent messages of any kind, designed to interfere with a user's terminal session, via any means, locally or by the Internet;
- using manual or electronic means to avoid any use limitations placed on the Services, such as timing out; or
- any 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.

Updates

Smarsh reserves the right to revise and update this AUP from time to time.

Current Version of AUP: Version 3, Effective June 1, 2015