Last Revised: February 1, 2019

BSM

ACCEPTABLE USE POLICY (AUP)

This is a legally binding agreement. Please read it carefully. This Acceptable Use Policy ("**AUP**") is part of the master software subscription, professional services and hardware purchase agreement between BSM (as defined below) and the Customer (the "**Master Agreement**").

For purposes of this AUP, "**BSM**" means the BSM entity named on the Order Form (either BSM Technologies Ltd. or BSM Analytics Inc.). Unless otherwise defined herein, capitalized terms used in this AUP have the meaning given in the Master Agreement.

1. Scope

This AUP applies to use of the Products by Customer and its Authorized Users.

2. Changes to AUP

BSM may change this AUP by posting an updated version of the AUP at www.bsmtechnologies.com/company/legal/agreement and such updates will be effective upon posting.

3. Violations of this AUP

A Customer's or Authorized Users violation of this AUP will be considered a material breach of the Master Agreement and/or other agreement governing Customer's use of the Products.

4. Use of Products.

Neither Customer nor its Authorized Users may:

- Interfere or attempt to interfere in any manner with the functionality or proper working of the Products;
- Upload to the Platform, or use the Products to store or transmit material in violation of third-party privacy rights;
- Upload to the Platform, or use the Products to store or transmit any malware. Malware means programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, or other malicious or unwanted software or programs;
- Use or permit the use of the Products to send unsolicited mass mailings outside its organization. The term "unsolicited mass mailings" includes all statutory or common definitions or understanding of those terms in the applicable jurisdiction, including without limitation, those set forth for "Commercial Electronic Mail Messages" under the U.S. CAN-SPAM Act;
- Upload, transmit or otherwise process any Protected Health Information (PHI) or any other regulated data or information in violation of any applicable law or regulation.
- Upload, transmit or otherwise process any Payment Card Information (PCI) in violation of any applicable Payment Card Information Security Standards or other similar requirements.

- Interfere with or disrupt the integrity or performance of the Products or third-party data stored or processed with the Products or attempt to gain unauthorized access to the Products or their related systems or networks; or

- Attempt to probe, scan, penetrate or test the vulnerability of a BSM system or network, or to circumvent, avoid or breach BSM's security or authentication measures, whether by passive or intrusive techniques, or by social engineering, without BSM's express prior written consent.

5. Shared Resources

Neither Customer nor its Authorized Users may use BSM systems, networks or technology in a way that unnecessarily interferes with their normal operation, or that consumes a disproportionate share of their resources. Customer agrees that BSM may quarantine or delete any data stored on BSM's systems or networks if BSM reasonably believes that the data is infected with any malware, or is otherwise corrupted, and has the potential to infect or corrupt BSM systems, networks or technology or other customers' data that is stored or accessed via BSM systems, networks or technology. Customer and its Authorized Users will comply with any written security or network access requirements that BSM provides to Customer in connection with its use of the Products.

6. Other Networks

Customer and its Authorized Users must comply with the rules of any other network its accesses or participates in when using the Products.

7. Abuse

Neither Customer nor its Authorized Users may use BSM's network or services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;

- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;

- Interference with service to any user of the BSM or other network including mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

- Use of an Internet account or computer without the owner's authorization;

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

- Collecting or using information without the consent of the owner of the information;

- Use of any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting;

- Use of the Products to distribute software that covertly gathers information about a user or covertly transmits information about the user;

- Any conduct that is likely to result in retaliation against the BSM network or website, or BSM's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS); or

- Use of the Products to facilitate competition with BSM, including through establishment of accounts that do not fairly represent their purpose, or for benchmarking purposes not authorized by BSM.

8. Offensive Content

Neither Customer nor its Authorized Users may publish, transmit or store on or via BSM's network or equipment any content or links to any content that BSM reasonably believes:

- is obscene;
- contains harassing content or hate speech, or is violent, incites violence, or threatens violence;
- is unfair or deceptive under the consumer protection laws of any jurisdiction;
- is defamatory or violates a person's privacy;
- creates a risk to a person's safety or health, creates a risk to public safety or health, is contrary to applicable law, or interferes with a investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- is intended to assist others in defeating technical copyright protections;
- infringes on another person's copyright, trade or service mark, patent, or other property right, or violates any privacy right;
- is illegal or solicits conduct that is illegal under laws applicable to you or to BSM; or
- is otherwise malicious, fraudulent, or may result in retaliation against BSM by offended viewers or recipients.

9. Other

Customer will not be entitled to any credit or other compensation for any interruptions of service resulting from AUP violations.