ACCEPTABLE USE POLICY

July 17, 2017 Revision
This Acceptable Use Policy can be found at
https://www.thinksis.com/legal

This ACCEPTABLE USE POLICY ("AUP") is incorporated by reference in the Data Center and Hosting Services Addendum ("Addendum") with SIS, which is part of the Master Services Agreement ("Agreement").

Coverage of this Policy
The following terms apply to Customer's use of and access to any SIS services or products ("Services") made available by SIS' Managed Solutions Center. Customer agrees to comply with this Acceptable Use Policy by using Services, which may be amended, modified or updated from time to time.

Customer Internal Use. Customer will ensure its end users will use the Services solely for its internal business purposes; and neither Customer nor its end users will: (i) commercially exploit the Services by licensing, sub-licensing, selling, re-selling, renting, leasing, transferring, distributing, time sharing or making the Services available in the manner of a service bureau; (ii) create derivative works based on the Services; (iii) disassemble, reverse engineer or decompile the Services or any part thereof or permit others to do so; or (iv) access all or any part of the Services in order to build a product or service that competes with the Services.

Illegal or Harmful Use. Customer will only use Services for lawful purposes. Customer bears all responsibility for ensuring its own users comply with all applicable laws and regulations and appropriate conduct, without limitation, outlined in this AUP.

Offensive, Harmful or Illegal Content. Customer may not publish or transmit via SIS's network and equipment any content or links to any content that SIS reasonably believes (i) is offensive and may be defamatory, obscene, abusive, excessively violent, threatening or harassing, invasive of privacy, objectionable or constitutes, fosters or promotes pornography; (ii) is harmful and is considered unfair or deceptive under consumer protection laws, such as pyramid schemes and chain letters, creates risks for a person or the public's safety or health, compromises national or local security, interferes with law enforcement investigations or improperly exposes trade secrets or other confidential or proprietary information of another person, or improperly exposes; or (iii) is illegal and may infringe upon another person's copyright, trade or service mark, patent, or other property right where permission was not first obtained by the owner of such rights, promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking, or is otherwise illegal or solicits conduct under laws applicable to Customer or SIS. Content "published or transmitted" via SIS's network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting or transmission that relies on the Internet.

Network Abuse. Customer may not use SIS's network to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including, (i) 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; (ii) monitoring data or traffic on any network or system without the express authorization of the owner of the system or network; (iii) user of an Internet account or computer without the owner's authorization, interfering with the service to any user of the SIS Service and network, including, without limitation, denial of service, mailing bombing or other flooding techniques to overload a system and broadcast attacks; (iii) collecting or using information without the consent of the owner of the information; (iv) use of any false, misleading, or deceptive TCP-IP packet header information to conceal the source or routing information of the network traffic or messages; (v) distributing software that covertly gathers information about or transmits information about a system or user; (vi) avoiding any limitations established by SIS using manual or electronic means to attempt to gain unauthorized access too, alter, or destroy information related to SIS or its Customers; (vii) any conduct

that is likely to interfere with, disrupt the integrity of or result in retaliation against the SIS network or website, or SIS's employees, officers or other agents.

Bulk or Commercial E-Mail. Customer must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial e-mail. Customer must not distribute, publish, or send through the SIS Network: (i) any spam, including any unsolicited advertisements, solicitations, commercial e-mail messages, informational announcements, or promotional messages of any kind; (ii) chain mail; (iii) numerous copies of the same or substantially similar messages; (iv) empty messages; (v) messages that contain no substantive content; (vi) very large messages or files that disrupt a server, account, newsgroup, or chat service; or (vii) any message that is categorized as "phishing."

Likewise, Customer may not: (i) participate in spidering, harvesting, or any other unauthorized collection of e-mail addresses, screen names, or other identifiers of others or participate in using software (including "spyware") designed to facilitate such activity; (ii) collect responses from unsolicited messages; or (iii) use any of the SIS mail servers or another site's mail server to relay mail, such as, bulk e-mail, without the express permission of SIS, the account holder or the site. SIS may test and otherwise monitor Customer's compliance with its requirements, and may block the transmission of e-mail that violates these provisions.

Security. SIS is responsible for maintaining the security of the infrastructure used to provision Services to Customer. It is the responsibility of the Customer to understand and evaluate the security responsibilities of each party for Services against its security requirements including compliance regulations. Customer must take reasonable security precautions during its use of Services to configure and protect its operating systems, applications and data. SIS does not assume responsibility or accountability for such protections unless additional Services are mutually defined between SIS and Customer. Customer is responsible for protecting the confidentiality of any accounts used in connection with Service and is encouraged to change associated passwords on a regular basis. Failure by the Customer to protect the assigned environment may result in a security compromise by an unauthorized source. A compromised server or network device is potentially disruptive to SIS's network and other customers. Therefore, SIS may, after notifying you of the situation, take Customer's server or other device off line if SIS determines that it is being accessed or manipulated by a third party without Customer's consent. Customer is solely responsible for the cost and resolution for any network or data breach introduced by Customer that affects systems, applications or data under Customer possession or control, or SIS networks and/or other SIS customers.

Vulnerability Testing. Customer may perform internal vulnerability assessments on IP addresses specific to the Customer instance at any time. These IP addresses are provided to the Customer at the time Services are on-boarded. With SIS' express written consent, Customers may perform external vulnerability assessments and penetration tests on those same Customer-designated IP addresses. Customer may not attempt to probe, scan, penetrate or test the vulnerability of a SIS system or network or to breach SIS's security or authentication measures, whether by passive or intrusive techniques that has not been specifically designated to the Customer by SIS for its use. SIS maintains the right to block or shut down any vulnerability testing technique regardless of consent that interferes with SIS networks and its Services.

Export Violations. Customer must comply with all applicable international and regional export laws and regulations in its use of Services. Customer agrees to not export or import software, technical information, data content, encryption software, or technology in violation of such export control laws. Customer represents and warrants that it is not located in, under the control of, or a national or resident of any country which the United States has a trade embargo or on an applicable government list.

Copyrighted Material. Copyright infringement is a serious matter. Customer may not use SIS's network or equipment to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image, or other work protected by copyright law unless, (i) Customer has been expressly authorized by the owner of the copyright to copy/use the work in that manner; (ii) Customer is otherwise permitted by established United States copyright law to copy/use the work in that manner. SIS may terminate Customer's service immediately if it is found to be infringing copyrights.

Copyright Infringement Notice (Digital Millennium Copyright Act). If Customer believes its copyright is being infringed by a person using the SIS network, please send your written notice of copyright infringement to:

Contracts and Compliance Department
SOFTWARE INFORMATION SYSTEMS, LLC
165 Barr Street
Lexington, KY 40507

Customer's notice must include the following:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
- Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single site are covered by a single notification, a representative list of such works at that site;
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit SIS to locate the material;
- Information reasonably sufficient to permit SIS to contact you, such as an address, telephone number, and, if available, an e-mail address;
- A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, the copyright owner's agent, or the law;
- A statement that the information in the notification is accurate, and under penalty of perjury that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Cooperation with Investigations and Legal Proceedings. SIS may, without notice to Customer report to the appropriate authorities any conduct by Customer that it believes violates applicable criminal law. SIS will attempt to notify Customer if SIS is requested to; provide any information it has about Customer in response to a formal or informal request from a law enforcement or government agency, or in response to a formal request in a civil action that on its face meets the requirements for such a request. Customer must understand that there may situations that will prevent SIS from making notification or preventing such data from being released without Customer's consent.

Other

- Customer must have valid and current information on file with its domain name registrar for any domain hosted on the SIS network.
- Customer may only use IP addresses assigned to it by SIS staff in connection with its SIS services.
- Customer agree that if the SIS IP numbers assigned to its account become listed on Spamhaus, Spews, NJABL or other abuse databases, you will be in violation of this AUP, and SIS may take reasonable action to protect its IP numbers, including suspension and/or termination of your Service, regardless of whether the IP numbers were listed as a result of your actions. Before taking any action to suspend or terminate Customer's service, SIS will investigate the matter and communicate with Customer regarding the possible causes of the problem and any reasonable actions that may be taken to absolve the IP numbers in question.

Consequences of Violation of AUP. SIS may without notice to Customer, suspend its service or remove any content transmitted via the SIS service if it discovers facts that lead it to reasonably believe Customer's service is being used in violation of this AUP. Customer must cooperate with SIS's reasonable investigation of any suspected violation of the AUP. SIS will attempt to contact Customer prior to suspension of network access to Customer's server(s), however, prior notification is not assured.

In the event SIS takes corrective action due to a violation of the AUP, SIS shall have no liability to Customer or to any of Customer's end users due to any corrective action that SIS may take (including, without limitation, suspension, termination or disconnection of Services).

Customer is strictly responsible for the violation of this AUP, including violation by its customers, users, and including violations that occur due to unauthorized use of Customer's service (but not including unauthorized use that results from SIS's failure to perform its obligations under the Agreement and Service Order Form).

SIS may charge Customer its hourly rate for AUP breach recovery (currently $200.00) plus the cost of equipment and material needed to (i) investigate or otherwise respond to any suspected violation of this AUP, (ii) remedy any harm caused to SIS or any of its customers by the violation of this AUP, (iii) respond to complaints, including complaints

under the Digital Millennium Copyright Act, (iv) respond to subpoenas and other third party requests for information as described in the Agreement, and (v) have SIS's Internet Protocol numbers removed from any abuse database. No credit will be available under Customer's SIS Service Level Objective for interruptions of service resulting from AUP violations.

Amendments to AUP. The Internet is still evolving, and the ways in which the Internet may be abused are also still evolving. Therefore, SIS may from time to time amend this AUP in accordance with its Agreement to further detail or describe reasonable restrictions on Customer's use of SIS' services. Inquiries regarding this policy should be directed to ATTN: Chief Information Security Officer of Information Security Department.

Disclaimer. SIS is under no duty, and does not by this AUP undertake a duty, to monitor or police our customers' activities and disclaims any responsibility for any misuse of the SIS network. SIS disclaims any obligation to any person who has not entered into an agreement with SIS for services.