ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**Policy**") sets out terms with which Customer must comply when using SISW's Cloud Services.

1. Definitions

Capitalized terms shall have the meaning given to them in the terms governing the Cloud Services.

2. No Illegal, Harmful, or Offensive Use of Customer Data

Customer shall not use, or encourage, promote, facilitate, or instruct others to use, the Cloud Services for any illegal, harmful, or offensive use. Customer Data must not be illegal, harmful, or offensive. In particular, Customer's use of the Cloud Services, Customer Data and Customer's use of Customer Data shall not:

(i) be in violation of any Laws or rights of others;

(ii) be harmful to others, or SISW's operations or reputation, including by offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi or pyramid schemes, phishing, farming, or other deceptive practices;

(iii) enter, store or send hyperlinks, enable access to external websites or data feeds, including embedded widgets or other means of access, in or as part of Customer Data, for which Customer has no authorization or which are illegal;

(iv) be defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable;

(v) subject SISW or its business partners to liability.

3. No violation of use restrictions

Customer shall not:

(i) copy, sell, resell, license, transfer, assign, sublicense, rent, lease, or otherwise make available the Cloud Services or the System in whole or in part to any third party (unless permitted otherwise by SISW or required by Laws);

(ii) translate, disassemble, decompile, reverse engineer or otherwise modify, tamper with, repair or attempt to discover the source code of any software contained in the Cloud Services or the System (unless permitted otherwise by SISW or required by Laws);

(iii) create derivative works of, or based on, any parts of the Cloud Services or the System;

(iv) change or remove any notices or notations from the Cloud Services or the System that refer to intellectual property rights or brand names;

(v) imitate the "look and feel" of any of SISW's website or other user interface, nor the branding, color combinations, fonts, graphic designs, product icons or other elements associated with SISW; and

(vi) upload to the System any of Customer Data that is subject to a license that, as a condition of use, access, and/or modification of such content, requires that any SISW's or SISW's business partners' software or service provided by SISW and interacting with or hosted alongside Customer Data: (a) are disclosed or distributed in source code form; (b) are licensed to recipients for the purpose of making derivative works; (c) are licensed at no charge; (d) are not used for commercial purposes; or (e) are otherwise encumbered in any manner.

4. No Abusive Use

Customer shall not do any of the following:

(i) use the Cloud Services in a way intended to avoid or work around any use limitations and restrictions placed on such Cloud Services, such as access and storage restrictions or to avoid incurring fees;

(ii) access or use the Cloud Services for the purpose of conducting a performance test, building a competitive product or service or copying its features or user interface or use the Cloud Services in the operation of a business process outsourcing or other outsourcing or a time-sharing service;

(iii) interfere with the proper functioning of any of SISW's systems, including any overload of a system by mail bombing, news bombing, broadcast attacks, or flooding techniques;

(iv) engage in any activity or modification or attempt to modify the System or the Cloud Services in such a way as to negatively impact on the performance of the System or the Cloud Services.

5. No Security Violations

Customer shall not use the Cloud Services in a way that results in, permits, assists or facilitates any action that constitutes a threat to the security of the System or the Cloud Services. Customer shall in particular:

(i) before accessing the Cloud Services, during use, and when transferring Customer's Data, take all reasonable precautions against security attacks on Customer's system, on-site hardware, software or Cloud Services that Customer uses to connect to and/or access the System, including appropriate measures to prevent viruses, trojan horses or other programs that may damage software;

(ii) not interfere with or disrupt the integrity or performance of the Cloud Services or other equipment or networks connected to the System, and in particular not transmit any of Customer Data containing viruses, trojan horses, or other programs that may damage software;

(iii) not use the Cloud Services in a way that could damage, disable, overburden, impair or compromise any of SISW's systems or their security or interfere with other Users of the System;

(iv) not perform any penetration test of or on the Cloud Services or the System without obtaining SISW's express prior written consent; and

(v) not connect devices to the Cloud Services that does not comply with industry standard security policies (e.g., password protection, virus protection, update and patch level).

6. Reporting

If Customer becomes aware of any violation of this Policy, Customer will immediately notify SISW and provide SISW with assistance, as requested by us, to stop, mitigate or remedy the violation.