DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “Agreement”) is entered into between Siemens Product Lifecycle Management Software Inc., also known as Siemens Industry Software (hereinafter referred to herein as “SISW”), and the customer that has signified its acceptance of the terms and conditions of this Agreement (“Customer”). SISW retains the right to utilize its affiliated companies in pursuing any of its rights and fulfilling any of its obligations under this Agreement. Therefore, the term “SISW” as used herein may also refer to affiliated companies that are directly or indirectly owned or controlled by the ultimate parent company of Siemens Product Lifecycle Management Software Inc. and who have been authorized by Siemens Product Lifecycle Management Software Inc. to distribute SISW cloud services (the “Cloud Service”).

Customer shall be solely responsible for determining the type of data and the individuals affected by the processing and shall ensure the legitimacy of such processing by means of the Cloud Service. Customer shall also be responsible for any correction, deletion or blocking of personal data, using the functionalities offered by the Cloud Service. Customer may export and delete its data, including personal data, using the functionalities offered by the Cloud Service. Upon termination of this Data Processing Agreement, Customer shall have 30 days to send a written request to SISW that Customer Data be made available for download by Customer. After expiration of any period set forth by SISW in response to such a request, any remaining data of Customer will be subject to deletion and will no longer be available to Customer. SISW and Customer agree that, within the scope of the Cloud Service, Customer’s right to issue instructions will be exercised exclusively by using the functionalities offered by the Cloud Service. Additional instructions concerning Customer’s data require a separate written agreement between SISW and Customer including an agreement on any additional fees to be paid by Customer for carrying out such instructions. Customer covenants that it will not upload or store any protected health information (PHI) in the Cloud Service, unless SISW and Customer have entered into a separate written agreement that expressly permits the storage of PHI in the Cloud Service.

In providing the Cloud Service, with respect to the production system, SISW shall comply with the technical and organizational measures described in Appendix 2 to Exhibit A of this Data Processing Agreement. Non-production systems related to the Cloud Service may or may not comply with the measures described in Appendix 2 to Exhibit A. In addition, SISW may change the technical and organizational measures applicable to the production system from time to time, provided that such changes do not adversely affect the level of protection afforded by such measures in any material way. SISW will restrict its personnel from collecting, processing or using personal data without authorization and will employ only personnel in processing of Customer’s personal data which have been specifically instructed in compliance with data privacy protection requirements.

SISW shall be entitled to engage subprocessors in the performance of the Cloud Service. To the extent access of subprocessors to Customer’s personal data cannot be excluded, SISW will provide to Customer upon request a list of such subprocessors and their respective locations and will update such list as required before any new subprocessor is granted access to Customer’s personal data. In case Customer reasonably objects to any new subprocessor, Customer shall inform SISW of such objection and, if SISW insists on the engagement of the new subprocessor, shall be entitled to terminate this Data Processing Agreement for good cause. To the extent that engagement of any such subprocessor involves a cross-border transfer of personal data, SISW will endeavor to cause such subprocessor to maintain an adequate level of data protection with respect to such personal data.

SISW will regularly verify adherence to the applicable technical and organizational measures and will, upon reasonable request by Customer, confirm to Customer that the applicable technical and organizational measures are adhered to. In case Customer has reason to believe that a confirmation issued by SISW is wrong, Customer shall be entitled to confirm adherence to the technical and organizational measures by scheduling an audit with SISW, subject to reasonable prior notice. Such audit shall be carried out at Customer’s cost and expense.

SISW and Customer agree that any data transfers of Customer’s personal data from countries in the European Union to countries outside the EU that the EU has deemed not to have adequate level of personal data protection will be conducted according to the provisions of the EU standard contractual clauses, which are set forth in Exhibit A and are fully incorporated herein. In the event of a conflict between the terms of this Data Processing Agreement and the terms of the standard contractual clauses, the provisions of the standard contractual clauses will prevail. The standard contractual clauses will be governed by the laws of the EU member state in which the data exporter (as defined in Exhibit A) is established.

Exhibit A
EU Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

by and between

Customer and/or an affiliate company of Customer based in the EU

(hereinafter, the "**data exporter**")

and

Siemens Product Lifecycle Management Software Inc., also known as Siemens Industry Software, including any affiliated companies that are directly or indirectly owned or controlled by the ultimate parent company of Siemens Product Lifecycle Management Software Inc. and who have been authorized by Siemens Product Lifecycle Management Software Inc. to process data on its behalf

(hereinafter, the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Section 1. Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Section 2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Section 3. Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Section 4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Section 5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Section 6. Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Section 7. Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

    (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Section 8. Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Section 9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Section 10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Section 11. Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Section 12. Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Customer is a subscriber to a Cloud Service provided by SISW, which permits end users authorized by Customer to enter, modify, use, remove, download, and otherwise process Customer Data, which may include personal data, as described in the Agreement and the relevant documentation for the Cloud Service.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Siemens Product Lifecycle Management Software Inc., by itself and/or through its subprocessors, provides the Cloud Service, which includes: maintaining computing infrastructure in the United States and European Union upon which the Cloud Service is operated; storing on the infrastructure Customer Data that is uploaded to the Cloud Service by Customer; monitoring the availability and ongoing operation of the Cloud Service and the infrastructure; and maintaining the security of the infrastructure as set forth in the Agreement and the relevant documentation for the Cloud Service.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Unless expressly specified in writing by the data exporter, data subjects may include end users authorized by Customer to use the Cloud Service and other personnel of Customer whose personal data is stored in the Cloud Service.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Specific data categories to be stored in the Cloud Service are subject to significant configuration by Customer, though some common categories of data that may be stored in the Cloud Service are, as non-limiting examples: name, email address, company name, telephone number, work location, nationality or citizenship, and information regarding access to and use of the Cloud Service. Depending on Customer’s configuration of the Cloud Service, many other data categories could be present in Customer Data.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Any special data categories to be stored in the Cloud Service would be as agreed between the parties in the Agreement or an Order, or as set forth in a statement of work for professional services to be provided to Customer as part of its deployment of the Cloud Service.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

The personal data may be processed: as part of the normal operation of the Cloud Service, depending on Customer’s configuration; through storage and/or archiving on the computing infrastructure maintained by data exporter, in single-tenant or multi-tenant environments; accessed or transmitted according to instructions issued to the Cloud Service by an end user authorized by Customer to use the Cloud Service; and as part of Cloud Service maintenance operations performed by data exporter.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Some Cloud Services offerings are provided under different terms, which if applicable will be set forth in an Order. Otherwise, the data importer will undertake the technical and organizational measures described below with respect to the personal data stored in the System, in accordance with Clauses 4(d) and 5(c) of the Clauses.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Physical Access Control. Unauthorized persons will be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process and/or use the personal data.

   Measures: All data centers adhere to strict security procedures enforced by security personnel, surveillance equipment, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all data centers:

   a. In general, buildings are secured through access control systems (smart card access system).
   b. Authorization credentials, which include an electronic access badge (unique to the employee, vendor, or contractor) and PIN—are provided to authorized personnel in order to physically access the data center facilities.
   c. Physical access to the data centers within the system boundary is enforced by an electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress.
   d. Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
   e. Access rights will be granted to authorized personnel on an individual basis according to the System and Data Access Control measures set out below. This also applies to visitor access. Guests and visitors to SISW buildings must register their names at reception and must be accompanied by authorized SISW personnel. SISW and all third party data center providers are logging the names and times of persons entering the private areas of SISW within the data centers.
   f. SISW employees and external personnel must wear their ID cards at all SISW locations.

2. System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

   Measures:
   a. SISW or its subprocessors manage the environment to comply with NIST SP 800-53 Rev 4 Access Control (AC) and Identification and Authentication (IA) requirements.
   b. Multiple authorization levels are used to grant access to sensitive systems including those storing and processing the personal data. Processes are in place to ensure that only authorized users have the appropriate authorization to add, delete, or modify users.
   c. All users access SISW's systems with a unique user name and a password that must meet certain minimum complexity criteria.
   d. SISW and its subprocessors have procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If an SISW user changes roles or leaves the company, a process is performed to revoke access rights to the environment.
   e. SISW and subprocessors have established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires regular changes to all user passwords, and requires default passwords to be changed. Personalized user IDs are assigned for authentication. All passwords must meet minimum complexity requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every 60 days that complies with the minimum complexity requirements. Each SISW computer has a password-protected screensaver.
   f. SISW or its subprocessors automatically audit the following account events: creation, modification, enabling, disabling, and removal. A system administrator reviews the logs periodically.
   g. Networks of SISW and its subprocessors are protected from the public internet by firewalls.

h. SISW and its subprocessors use up–to-date antivirus software at access points to the company network, for e-mail accounts, and on all file servers and all workstations.
i. SISW and its subprocessors implement security patch management to ensure deployment of relevant security updates.
j. Full remote access to SISW's corporate network and critical infrastructure is protected by strong, multi-factor authentication.

3. Data Access Control. Personnel entitled to use data processing systems will gain access only to the personal data that they have a right to access, and the personal data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:
a. Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SISW uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the SISW security policies and standards.
b. All production servers of any SISW Cloud Service are operated in the relevant data centers. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SISW also incorporates periodic external audits to confirm these measures are applied in appropriate fashion.
c. SISW does not allow the installation of personal software or other software not approved by SISW to systems being used for any Cloud Service.
d. Should there be a requirement to transfer data due to the failure of underlying data storage media, upon completion of such transfer, the failed storage media will either be degaussed (for magnetic storage) or shredded (for solid-state or optical storage).

4. Data Transmission Control. Personal data must not be read, copied, modified or removed without authorization during transfer.

Measures:
a. SISW or its subprocessor will manage the infrastructure and configuration to comply with NIST SP 800-53 Rev 4 Systems and Communication Protection (SC) requirements. This includes network-based intrusion prevention systems (NIPS) and firewalls at system boundaries to protect against malicious communications at the external boundary of the infrastructure. NIPS and firewalls are configured per DISA STIG standards. Data is encrypted in transit using cryptographic modules that comply with FIPS 140-2.
b. Where data carriers are physically transported, adequate measures are implemented at SISW to ensure the agreed service levels (for example, encryption, and lead-lined containers).
c. Transmission of the personal data over SISW internal networks is protected in the same manner as any other confidential data according to SISW's security policies.
d. When the data is transferred between SISW and Customer, the protection measures for the transferred personal data are as set forth in the Agreement or the relevant documentation for the Cloud Service. This applies to both physical and network based data transfer. Customer assumes responsibility for any data transfer from SISW's Point of Demarcation (e.g. outgoing firewall of the data center which hosts the Cloud Service).

5. Data Input Control. The Cloud Service will permit retrospective determination whether and by whom personal data has been entered, modified or removed from the infrastructure used to provide the Cloud Service.

Measures:
a. SISW only allows authorized personnel to access the personal data as required in the course of their work. SISW implemented a logging system for input, modification and deletion, or blocking of personal data by SISW or its subprocessors to the greatest extent supported by the Cloud Service.
b. Audit trails provide sufficient detail required to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected. Each operating system event log record includes the event type, a time stamp, the event source, the event location, the outcome of the event, and the user associated with the event.

6. Job Control. Personal data will be processed solely in accordance with the terms of the Agreement and any related instructions provided by Customer.

Measures:

a. SISW uses controls and processes to ensure compliance with contracts between SISW and its customers, subprocessors, or other service providers.
b. Customer Data will be subject to at least the same protection level as confidential information according to the SISW Information Classification standard.
c. All SISW employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SISW customers and partners.

7. Availability Control. Personal data will be protected against accidental or unauthorized destruction or loss.

Measures:

a. SISW employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
b. SISW relies on global cloud service providers to ensure power availability to data centers.
c. SISW has defined contingency plans as well as business and disaster recovery strategies for Cloud Services.

8. Data Separation Control. Personal data collected for different purposes can be processed separately.

Measures:

a. When applicable, SISW uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between personal data of Customer and that of any other customer.
b. SISW maintains dedicated instances (with logical or physical separation) for each customer.
c. Customer (including its Affiliates) has access only to its own customer instance(s).

9. Data Integrity Control. Ensures that the personal data will remain intact, complete, and current during processing activities:

Measures: SISW has implemented a defense strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above. The configuration of firewalls will result in multiple network segments that separate public and private access. Each firewall rule set will have specific access controls specifying the allowed communications between these segments.

a. Security Monitoring Center: Automated intrusion detection software will be used in conjunction with other security prevention and forensics software and process to alert, investigate and if required, notify and assist in the remediation of any security incident.
b. Antivirus software: all systems will have current antivirus definitions configured to protect against virus, worms, trojans, and other forms of malware.
c. Backup and recovery: all systems will have a base level of backup snapshots of data and configuration. If applicable, SISW and its subprocessors will also operate a customer’s instance with high availability configuration that will ensure that data is stored in two separate data centers of sufficient distance from each other.
d. Regular external audits to prove security measures. SISW and its subprocessors will undergo periodic external audits to test the security measures listed above.