GENERAL DATA PROTECTION TERMS

Article 1 General

1.1 Siemens Product Lifecycle Management Software Inc., or one of its Siemens Industry Software affiliated companies (collectively referred to herein as "**SISW**") has entered into a software license and services agreement with the Customer for Software, which may have taken the form of a written agreement signed by both parties or a click-wrap or online agreement agreed to by Customer electronically (referred to herein as the "**Agreement**"). These terms and conditions (the "**Terms**") are specific to the Services. These terms are additional to the terms in the Agreement and, to the extent that these terms are in conflict with the terms of the Agreement, these terms will take precedence and supersede the terms of the Agreement with respect to the Services.
1.2 Capitalized terms shall have the meaning given to them above or in Article 12 and otherwise shall have the meaning given to them in the Agreement.

Article 2 Purpose and scope

2.1 These Terms serve as a commissioned data processing agreement between Customer and SISW and apply to the Services. They constitute Customer's and SISW's data protection related rights and obligations with regard to the Services. All other rights and obligations shall be exclusively governed by the other parts of the Agreement.
2.2 In providing the Services, SISW shall observe all data protection laws and regulations applicable to Processors and shall Process Personal Data only in accordance with the terms of the Agreement (including these Terms). Customer shall be responsible for compliance with any laws and regulations applicable to Customer (especially laws and regulations applicable to Controllers) and shall ensure that SISW and its Sub-Processors are allowed to provide the Services as Processor or Sub-Processor.

Article 3 Details of the Processing conducted by SISW

3.1 SISW shall conduct the Processing set out in Articles 3.2 to 3.4 below in the provision of the Services provided that the parties may provide further details for a particular service in an LSDA, SOW or other agreed transaction document.
3.2 In providing the Services, SISW may Process Personal Data when performing (i) software installation, maintenance services and/or professional services which may require (a) user account creation or access to personal information in customer networks, either on premise or remote, (b) transfers and uploads of Customer files and screen sharing which may contain personal data.
3.3 The data subjects for the purposes of the Processing shall include employees, contractors, business partners or other individuals whose Personal Data is subject to Processing.
3.4 The Customer shall determine the categories of Personal Data that will be subject to the Processing in connection with the Services. The Personal Data subject to the Processing may include, name, email address, time zone, location, company name, office address, phone number and any other Personal Data that the Customer may provide in connection with the Service, provided that the Services are not intended for the Processing of special categories of Personal Data and the Customer shall not transfer directly or indirectly any such sensitive data to SISW.

Article 4 Instruction rights

4.1 As Processor SISW shall only Process Personal Data upon Customer's documented instructions. The Agreement (including these Terms) constitutes Customer's complete and final instructions for the Processing of Personal Data by SISW as Customer's Processor. Any additional or alternate instructions must be agreed between SISW and Customer in writing and may be subject to additional costs. SISW shall inform Customer if, in the opinion of SISW, an instruction infringes applicable data protection law. SISW shall, however, not be obligated to perform any legal examination of Customer's instructions.
4.2 SISW shall rectify, erase or restrict the Processing of Personal Data as instructed by Customer.

Article 5 Technical and organizational measures

5.1 SISW shall implement the Measures described in Annex 1. Customer hereby confirms that the level of security provided is appropriate to the risk inherent with the Processing by SISW on behalf of Customer.
5.2 Customer understands and agrees that the Measures are subject to technical progress and development. In that regard, SISW shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

Article 6 Commitment to confidentiality

6.1 SISW shall ensure that personnel engaged in providing the Services shall maintain the confidentiality of Personal Data.

Article 7 Sub-Processors

7.1 Customer hereby approves the engagement of any affiliates of SISW and any other Sub-Processors agreed in accordance with Article 3.1 in any LSDA, SOW or other transactional document. SISW shall enter into a contract with each Sub-Processor imposing appropriate contractual obligations on the Sub-Processor that are no less protective than these Terms and provide a copy of the respective agreement upon Customer's written request, redacted for commercial or otherwise confidential information.
7.2 SISW shall be authorized to remove or add new Sub-Processors. New Sub-Processors shall be approved by Customer (such approval not to be unreasonably withheld or delayed) in accordance with the following process:
(i) SISW shall notify the Customer with at least ten (10) days prior notice before authorizing any new Sub-Processor to access Customer's Personal Data.
(ii) If Customer raises no reasonable objections with SISW in writing within this ten (10) days period, then this shall be taken as an approval of the new Sub-Processor, provided SISW informed Customer in the notification about such consequence.
(iii)If the Customer raises objections vis à vis SISW, then SISW shall have the right to terminate the relevant Services with ten (10) days' notice unless SISW chooses in its discretion to (a) continue the Service without the engagement of the Sub-Processor which Customer objected to or (b) take sufficient steps to address the concerns raised in Customer's objection
7.3 SISW shall remain fully liable to Customer for the performance of the Sub-Processor's obligations. However, SISW shall not be liable for damages and claims that ensue from Customer's instructions to Sub-Processors.

Article 8 Non-EEA and Privacy Shield Certified Sub-Processors

8.1 In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA or Switzerland, this Article 8 shall apply and SISW shall implement the Transfer Safeguards identified per Sub-Processor in the respective LSDA, SOW or other transactional document agreed in accordance with Article 3.1. It is Customer's responsibility to assess whether the respective Transfer Safeguard implemented suffices for Customer and Further Service Recipients (if any) to comply with applicable data protection law.
8.2 If a Transfer Safeguard is based on the EU Model Contract, SISW shall enter into such EU Model Contract with the relevant Sub-Processor. Each EU Model Contract shall contain the right for Customer and Further Service Recipients (if any) located within the EEA or Switzerland to accede to the EU Model Contract. Customer hereby accedes to the EU Model Contracts (as a data exporter) with current Sub-Processors and agrees that its approval of future Sub-Processors in accordance with Section 7.2 shall be deemed as declaration of accession to the EU Model Contract with the relevant future Sub-Processor. Furthermore, Customer agrees to procure assent from each of its Further Service Recipients (also as data exporters) to accede to such EU Model Contracts. SISW hereby waives (also on behalf of the respective Sub-Processor) the need to be notified of the declaration of accession of Customer or Further Service Recipients.
8.3 If a Transfer Safeguard is based on the Privacy Shield or Processor Binding Corporate Rules then SISW shall contractually bind such Sub-Processor to comply, as the case may be, with the principles of its Privacy Shield certification or its Processor Binding Corporate Rules.

Article 9 Notification obligations and SISW support

9.1 After having become aware of it, SISW shall notify Customer without undue delay of any Personal Data Breach. SISW shall (i) reasonably cooperate with Customer in the investigation of such Personal Data Breach, (ii) provide reasonable support in assisting Customer in its security breach notification obligations under Applicable Data Protection Law (if applicable) and (iii) initiate respective and reasonable remedy measures.
9.2 SISW shall notify Customer without undue delay of (i) complaints or requests of data subjects whose Personal Data is Processed pursuant

the Terms or (ii) orders or requests by a competent supervisory authority or court.
9.3 At Customer's request and at the Customer's reasonable expense, SISW shall reasonably support Customer in: (i)
dealing with complaints, requests or orders described in Article 9.2; and (ii) fulfilling its obligations under Applicable Data Protection Law.

Article 10 Audits

10.1 Customer shall have the right to audit, in accordance with Articles 10.2 to 10.4 below, SISW's and Sub-Processors' compliance with the data protection obligations hereunder annually (in particular in regard to the Measures implemented), unless additional audits are necessary under applicable data protection law; such audit being limited to information and data processing systems that are relevant for the provision of the Services provided to Customer.
10.2 SISW and Sub-Processors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. In such case each audit may result in the generation of an audit report. Where a control standard and framework implemented by SISW or our Sub-Processors provides for audits, such audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Upon Customer's request, SISW shall provide any relevant information in connection with its data protection obligations from such audit reports and corresponding information (together "**Audit Reports**") for the Services concerned.
10.3 Customer agrees that these Audit Reports shall first be used to address Customer's audit rights under these Terms. In case Customer can demonstrate that the Audit Reports provided are not reasonably sufficient to allow Customer or a Further Service Recipient to comply with the applicable audit requirements and obligations under applicable data protection law, Customer or Further Service Recipient shall specify the further information, documentation or support required. SISW shall render such information, documentation or support within a reasonable period of time at Customer's expense.
10.4 The Audit Reports and any further information and documentation provided during an audit shall constitute SISW Confidential Information and may only be provided to Further Service Recipients pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Sub-Processors, Company and Further Service Recipients may be required to enter into non-disclosure agreements directly with the respective Sub-Processor before issuing Audit Reports to Company or Further Service Recipients

Article 11 Termination

11.1 Upon termination of the Services, unless otherwise agreed between the parties, SISW shall erase all Personal Data made available to SISW or obtained or generated by SISW on behalf of the Customer in connection with the Services, unless required to retain in accordance with applicable law. The erasure shall be confirmed by SISW in writing upon request.

Article 12 Definitions

12.1 "**Adequacy Decision**" shall mean a decision by the European Commission in the meaning of Article 45 GDPR that a country outside the EEA ensures an adequate level of protection with respect to Personal Data.
12.2 "**Agreement**" means the agreement between SISW and Customer.
12.3 "**Applicable Data Protection Law**" means the legislation protecting the right to privacy with respect to the Processing of Personal Data (for example GDPR).
12.4 "**Controller"** means Customer and, as the case may be, further Service Recipients which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data.
12.5 "**EEA**" means the European Economic Area.
12.6 "**EU Model Contract**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 or any successor agreement issued by the European Commission.
12.7 "**Further Service Recipient**" means any third party (such as an affiliated company, branch, or other related entity of Customer) which is entitled to receive Services under the terms of the Agreement.
12.8 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
12.9 "**Measures**" means technical and organizational measures for the protection of Personal Data.
12.10 "**Personal Data**" has the meaning given to that term in Art 4 (1) GDPR and, for the purposes of these Terms, includes only such Personal Data Processed by SISW as Customer's Processor and in any event shall not constitute Customer Confidential Information for the purposes of the Agreement.
12.11 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under these Terms.
12.12 "**Privacy Shield**" means, with regard to Controllers located within the EEA, the European Union / United States Privacy Shield arrangement or, with regard to Controllers located in Switzerland, the Switzerland / United States Privacy Shield arrangement.
12.13 "**Processor**" means a natural or legal person, which Processes Personal Data on behalf of a Controller.
12.14 "**Processor Binding Corporate Rules"** means binding corporate rules in the meaning of Article 47 GDPR implemented in a group of companies that apply to Personal Data received from a Controller established in the EEA and/or Switzerland which is not a member of the group and then processed by the group members as Processors and/or Sub-Processors.
12.15 "**Processing**" has the meaning given to that term in Art. 4 (2) of the GDPR.
12.16 "**Services**" means services provided under the Agreement that involve the Processing of Personal Data by SISW acting in its role as Processor for Customer and/or Further Service Recipients acting as Controllers. The Services are further specified in Article 3.
12.17 "**Sub-Processor"** means any further Processor engaged by SISW in the performance of the Services provided under the terms of the Agreement and these Terms. Sub-Processor shall only mean a subcontractor with access to Personal Data.
12.18 "**Transfer Safeguards**" means (i) an Adequacy Decision or (ii) appropriate safeguards as required by Article 46 GDPR.
12.19 "**Transfers to Non-EEA Recipients**" means (i) the Processing of Personal Data outside the EEA (excluding a country with an Adequacy Decision) or (ii) any access to Personal Data from outside the EEA (excluding a country with an Adequacy Decision) by SISW or any of its Sub-Processors.

Annex 1
Technical and organizational Measures pursuant to Art. 32 GDPR

I. **Introduction**
This document describes the Measures which SISW shall implement as a minimum in connection with the Processing of Personal Data carried out by SISW, taking into account the state of the art in technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
If different, special measures are agreed in the LSDA, SOW or other agreed transaction document, those special measures apply instead of or in addition to the Measures.

II. **Basic Measures**
The basic Measures assure the protection of confidentiality and the integrity of the systems with which SISW processes Personal Data, especially by way of remote access. These Measures apply for all Processing carried out by SISW unless agreed otherwise in the LSDA, SOW or other agreed transaction document.
1. **Internal organization of operations**
SISW has appointed a company data protection manager. All employees and service providers of SISW that have access to Personal Data are under obligations to process this data only upon instruction and exclusively for the performance of the contractually agreed Services.
2. **Protection against unauthorized access**
Unauthorized persons must be prevented from entering the computer centers or business premises in which data Processing takes place.
Measures:
SISW shall protect the buildings or business premises with reasonable control systems for physical access based on the security classifications of the buildings or business premises and correspondingly defined entry authorization concepts. All buildings or business premises must be secured with technical entry control Measures e.g. using a card reading system. Depending on the security classification, real property, buildings or individual areas must be secured with additional Measures. This can include special profiles for physical entry, biometrics, pin-pads and turnstile systems to allow only individual entry, video surveillance and security personnel.

Rights to enter for authorized persons are issued individually in accordance with established criteria. This also applies with regard to external persons.

3. **Protection for computers**
The computers used for the Processing must be secured and protected against unauthorized use.
Measures:
Only authenticated users receive access to computers (e.g. notebooks, workstations) using, for example, the following Measures: data encryption, individualized issuance of passwords (compliant with standard industry practices such as at least 8 characters, normally with automatic expiration), employee identity cards with personal identity encryption, automatic lock-down of inactive systems. The protection of the used computers against attacks as well as accidental or intentional destruction or modification is provided, among other Measures, by intrusion detection systems, firewalls and regularly updated malware filters.
4. **Protection of data upon transmission, transport and remote access**
Care must be taken that Personal Data cannot be read, copied, changed or removed during electronic transmission or during the transport of the data or storage of it on data media and that it is possible to examine and determine at which places a transmission of Personal Data was made.
Measures:
The electronic communication channels must be secured with the installation of secured networks and processes for data encryption. In the case of physical transport of data media, data will be protected by encryption. Data media must be disposed of in a manner appropriate for protection of sensitive data. Remote maintenance connections must be protected by means of encryption. The date, type and scope of the remote maintenance must be recorded in auditable log data files.

III. **Specific Measures for Services in which Siemens stores customer data in IT systems**
These specific Measures assure the protection of the confidentiality, integrity, availability and resilience of the IT systems in which Siemens stores customer data. These Measures apply when the storage of data represents a material aspect of the contractual Services by Siemens and is not just temporary.
1. **Protection against unauthorized Processing**
There must be assurance that the persons authorized to use an IT system exclusively can access the data subject to their access authorization and that Personal Data cannot be read, copied, changed or removed without authorization during the Processing, use and during storage.
Measures:
Access to Personal Data in IT systems is granted on the basis of an authorization concept based on the function being performed ("need to know"). Furthermore, unauthorized access to Personal Data is prevented as needed by means of data encryption.
2. **Assurance of traceability**
There must be assurance that it is possible to subsequently examine and determine whether and by whom Personal Data has been entered, changed or removed in data Processing systems.
Measures:
SISW only permits authorized users to have access to Personal Data on the basis of a "need to know" authorization concept. Access to Personal Data is entered in log data files which record in detail in a protocol, the production, modification and removal of Personal Data.
3. **Assurance of integrity, availability and resilience**
There must be assurance that the systems used for the Processing are secured against failure and that Personal Data is available and protected against loss.
Measures:
SISW stores Personal Data by using redundant systems, depending on the security classification. SISW also uses interruption-free electric power (e.g. UPS, batteries, generators) to secure the supply of electric power in SISW's computer centers. A comprehensive, written disaster recovery plan must be prepared. Disaster recovery procedures and systems are regularly tested.