Supplemental Terms for SINEMA Remote Connect as a Service

These Supplemental Terms set out additional terms and conditions for the subscription to SINEMA Remote Connect as a Service Offering as described in the Documentation (2.3) and amend the Universal Customer Agreement ("UCA") between Customer and Siemens solely with regard to this SINEMA Remote Connect as a Service Offering. These Product-Specific Supplemental Terms form together with the UCA and other applicable Supplemental Terms the agreement between the parties ("**Agreement**").

1. GENERAL

1.1. Order of Precedence

In case of inconsistencies between the Order, the UCA and these Product-Specific Supplemental Terms, the following order of precedence shall apply in subordinate order:

(i) Order
(ii) Supplemental Terms for SINEMA Remote Connect as a Service
(iii) Additional referenced Annexes
(iv) UCA

1.2. Definitions

The following additional definitions apply to these SINEMA Remote Connect Service Supplemental Terms:

"**Affiliate**" means any entity that controls, is controlled by, or is under common control with Customer; in this context, "control" means ownership, directly or indirectly, of a majority of the outstanding equity of an entity.

"**Authorized Agen**t" means an individual who requires access to the Offering in support of Customer's or Customer Affiliates' internal business as consultant, agent, or contractor.

"**Authorized User**" means all Customer's and its Affiliates' employees or Authorized Agents.

"**High Risk System**" means a Service Item that requires or has incorporated enhanced safety functionalities such as fail-safe or fault-tolerant features to maintain a safe state where it is reasonably foreseeable that failure of the Service Item could lead directly to death, personal injury, or cata-strophic property damage. High Risk Systems may be required in critical infrastructure, direct health support devices, aircraft, train, boat, or vehicle navigation or communication systems, air traffic control, weapons systems, nuclear facilities, power plants, medical systems and facilities, and transportation facilities.

"**Server**" is the device on which the SINEMA Remote Connect Management Software operates.

"**Service Item**" means any physical device that is configured in the SINEMA Remote Connect Management Software to upload data to or exchange data with an Authorized User.

"**SINEMA Remote Connect Client Software**" is the Software that is required to connect a Windows based computer with the Server.

SINEMA Remote Connect Edge Client Software" is the Software that is required to connect any kind of EDGE device to the Server.

"**SINEMA Remote Connect Management Software**" means the software contained within the SINEMA Remote Connect as a Service offering.

"**Territory**" is linked to the geographical position of an Authorized User and to the geographical position of a Service Item and means worldwide (subject to Customer's obligations in the Agreement regarding compliance with export controls) unless a geographic area is specified on the Order.

"**User Account**" means a specific user account that is created in the SINEMA Remote Connect Management Software.

"**VPN Connection**" means (1) a VPN connection between a Service Item and the Server that is pre-configured within the SINEMA Remote Connect Management Software and (2) a VPN connection between the Server and an User Account that is pre-configured within the SINEMA Remote Connect Management Software.

2. USE OF THE OFFERING

2.1. Authorized Access and Use

Notwithstanding Section 3.1 and 3.3 of the UCA and unless otherwise defined in the Entitlements the SINEMA Remote Connect as a Service Offering may be accessed and used by Authorized Users in accordance with the Entitlements in the Territory for the Subscription Term, solely for Customer's or its Affiliates' internal use to provide services to third parties.

2.2. Entitlement

Different options of the SINEMA Remote Connect as a Service Offering are available. Customer is only authorized to use the SINEMA Remote Connect as a Service Offering in accordance with the size to which Customer holds a valid subscription. The sizes in the table below have limits that apply for the entire Subscription Term.

Options	S	M	L
Maximum number of VPN Connections	64	256	1024
Maximum number of SINEMA Remote Connect Client Software instances	10	32	60
Maximum number of Sinema Remote Connect Edge Client Software instances	5	20	50

2.3. Documentation.

The specifics of the SINEMA Remote Connect as a Service Offering and the Entitlements are described in the Documentation available at [https://support.industry.siemens.com/cs/ww/de/view/109823836] which is incorporated herein by reference. Documentation includes information such as applicable limits or other attributes and metrics of the available Options, prerequisites of the SINEMA Remote Connect as a Service Offering and additional third-party terms which prevail for third-party software, technology, data and other materials, including open source software licensed from third parties.

2.4. Restrictions for use of VPN technology and corresponding obligations of customer

Customer acknowledges that the use of VPN technology or any means for secured remote login, remote engineering, or data transfer in connection with the use of the SINEMA Remote Connect as a Service Offering may only be used by the Customer if the Customer is the owner of the system or data that is accessed or transferred by the SINEMA Remote as a Service Offering or if the Customer is legally

authorized by the owner of such systems or data to have them accessed or transferred by the SINEMA Remote as a Services Offering. Customer acknowledges further that the use of the SINEMA Remote Connect as a Service Offering may be subject to local restrictions or prohibitions including but not limited to those regarding encryption (e.g. use of tunnels), data sensitivity (e.g. production-related data), or cross-border traffic in certain countries. It is Customer's responsibility to check if such local restrictions or prohibitions apply and to use the SINEMA Remote as a Services Offering in compliance with applicable law.

3. DATA PRIVACY

3.1. Applicable Terms

For this SINEMA Remote Connect as a Service Offering the Additional Data Privacy Terms Annex (including list of Subprocessors) at

https://www.siemens.com/global/en/company/about/compliance/dataprivacy/dataprivacyterms/di-subprocessors.html applies.

3.2. Location of Data Centers

Customer Content at rest will be stored within the European Union.

4. SUBSCRIPTION TERMS/RENEWALS

The Subscription Term for the SINEMA Remote as a Services Offering is 12 months. The Subscription Terms ends automatically.

5. SERVICE LEVELS

5.1. Service Level

Siemens will use commercially reasonable efforts to make the SINEMA Remote Connect as a Service Offering available to Customer up to 24 hours per day and 7 days a week excluding downtime resulting directly or indirectly from any SLA Exclusions. The Cloud Services are available to Customer if its user interface is accessible by login at the exit of the wide area network of the data center used by Siemens to provide the SINEMA Remote Connect as a Service Offering.

5.2. Service Level Exclusions ("SLA Exclusions")

Service level commitments exclude downtime resulting directly or indirectly from any SLA Exclusions. SLA Exclusions" means unavailability or any other performance issue causing downtime of the Cloud Services as a result of:

(i) scheduled and communicated maintenance;
(ii) downtime for which at least 24 hours prior notice is provided to Customer;
(iii) factors outside Siemens' reasonable control;
(iv) actions or inactions of Customer or any third party;
(v) any equipment, software or other technology not provided by Siemens; or
(vi) suspension or termination of Offerings in accordance with the Agreement

5.3. Prerequisites and Schedule for the provision of Updates

The Customer will be notified by Siemens that a new update for the SINEMA Remote Connect Management Software is available to the email address information provided by the Customer. In the notification a minimum of 2 possible maintenance windows are communicated in which the update can be performed by Siemens. The Customer can choose one of these windows. If the Customer does not react to the inquiry, the update of the SINEMA Remote Connect Management Software will be performed by Siemens in the last offered maintenance window.

Possible maintenance windows will be communicated at least one week in advance.

In case of a security critical update which requires urgent action, the update of the SINEMA Remote Connect Management Software can be performed by Siemens after a 24-hour prior notice according to paragraph 5.2 (ii).

The customer also has the option to perform the update of the SINEMA Remote Connect Management Software at any given time prior to the last offered maintenance window on its own. A description on how to perform the update will be provided by Siemens, e.g. via Siemens Industry Online Support portal.

After successful update, the Customer will be informed via email.

Prerequisites:

The Customer needs to provide up-to-date email address information within the order process of the SINEMA Remote Connect as a Service Offering. The Customer needs to inform Siemens about any changes to this information.

5.4. Backup Functionalities

Backups of the server instance will be performed cyclically by Siemens once a week as well as prior to an update of the SINEMA Remote Connect Management Software. Backups will be retained for a period of three months.

The internal backup functionality of SINEMA Remote Connect Management Software can be used by the customer. However, the settings in the “Backup & Restore” menu must not be changed. This includes “Maximum number of local backup copies”, “Automatic backup interval” and “Coding key”. The configured Coding key is securely stored by Siemens and initially delivered to the Customer.

6. TECHNICAL SUPPORT

6.1. Contact

Customer may contact Siemens’ Technical Support organization as primary point of contact for support in relation to the Offering. All Support inquiries must be made through:

https://support.industry.siemens.com/cs/my/src

6.2. Scope of Technical Support

Subject to availability Siemens offers Customer support services Monday to Friday, 8am to 5:00pm (CET, CEST), excluding national and local holidays in Germany. Siemens will respond to Customer's

support inquiry at Siemens' sole discretion via e-mail, hotline or remotely as described in this clause. Customer must ensure remote access to its local networks for e.g. remote diagnoses. The following types of incidents are excluded from the scope of support, but Customer may revert such requests to the sales team(s) for resolution:

- incidents regarding a release, version, and/or functionalities of a service developed or configured specifically for Customer (unless otherwise expressly set forth in an Order);
- incidents ascribed to a consulting or training request ("how-to"). These are covered by the online user documentation;
- incidents ascribed to a custom development request.

The Technical Support is available in English and German.
To receive support services hereunder, Customer shall reasonably cooperate with Siemens' Support to resolve support incidents and shall have adequate technical expertise and knowledge of its configurations to provide relevant information to enable Siemens' Support to reproduce, troubleshoot and resolve the experienced error such as, by way of an example, instance name, username, form name and screenshot. Such support services may require that Siemens gets access to Customer content in which case, Customer is required to issue temporary credentials to Siemens to permit that access. By default, a dedicated service account is created for this purpose.

7. NOTICES

Notwithstanding Section 13.7 of the UCA, notices to Siemens shall be sent to sinema_rc_as_a_service.industry@siemens.com

8. PROHIBITED HIGH RISK USE

Customer acknowledges and agrees that (i) the SINEMA Remote Connect as a Service Offerings are not designed to be used for the operation of or within a High Risk System if the functioning of the High Risk System is dependent on the proper functioning of the SINEMA Remote Connect as a Service Offering and (ii) the outcome from any processing of data through the use of the SINEMA Remote Connect as a Service Offering is beyond Siemens' control. Customer will indemnify Siemens, its Affiliates, its subcontractors, and their representatives, against any third party claims, damages, fines and cost (including attorney's fees and expenses) relating in any way to any use of an SINEMA Remote Connect as a Service Offering for the operation of or within a High Risk System.

9. IT-SECURITY

Unless otherwise stipulated in the Documentation, the following shall apply with regard to security: Siemens maintains a formal security program that is designed to protect against threats or hazards to the security of Customer Content. Providers of Siemens' cloud infrastructure are required to (i) implement and maintain a security program that complies, inter alia, with ISO 27001 or a successor standard (if any) that is substantially equivalent to ISO 27001 and that is designed to provide at least the same risk management and security controls as evidenced by the certification of the providers under ISO 27001 and (ii) have the adequacy of their security measures annually verified by independent auditors. Siemens' cloud infrastructure (i) employs firewalls, anti-malware, intrusion detection/prevention systems (IDS/IPS), and corresponding management processes designed to protect service delivery from malware and (ii) is operated under a security governance model aligned with ISO 27001. This

Section contains Siemens' entire obligation regarding the security of Customer Content and the cloud infrastructure for the SINEMA Remote Connect as a Service Offering.

10. SECURITY DISCLAIMER

In order to avoid circumstances or events with the potential to adversely impact Customer's and/or Customer's Affiliates' plants, systems, machines and networks via unauthorized access, destruction, disclosure and/or modification of information, denial of service attacks or comparable scenarios (so-called "Cyberthreats"), it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. While the Industrial Edge Offerings are designed with security functions in mind which support secure industrial operations, Siemens' products and solutions only form one element of such a concept and it is up to Customer and Customer's Affiliates to configure these functions. Consequently, Customer and Customer's Affiliates remain responsible to prevent unauthorized access to its plants, systems, machines and networks and Siemens disclaims all liability for damage resulting from such Cyberthreats to the maximum extent permitted by law. Such systems, machines and components should only be connected to the enterprise network or the internet once a month to receive updates but only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. Customer and Customer's Affiliates are advised to take Siemens' guidance on appropriate security measures into account, which can be found at https://www.siemens.com/industrialsecurity. In this respect updates to the Offerings should be applied as soon as available and the newest version of the Offering should be used, since use of versions that are no longer supported and failure to apply updates may increase exposure to Cyberthreats.