

ADDENDUM ON REMOTE ACCESS TO GENERAL TERMS AND CONDITIONS OF SALES - SIEMENS, S.A. FOR MAINTENANCE/SERVICE (VERSION OF 06/2019) ("GTR")

1. Scope

1.1 Siemens, S.A. (hereinafter "**Siemens**") is authorized by Customer to maintain, calibrate and/or repair Customer's security, fire, building and/or automation systems ("**Systems**") via remote access ("**Remote Access**") as agreed between the Parties. Such maintenance and services may comprise the service and maintenance of the System itself, its components (hardware and software), and calibration/optimization of the System ("**Remote Services**").

1.2 The GTR shall serve as an addendum to the "Terms and Conditions of Sale – Siemens S.A." and/or any other agreement in place between Siemens and Customer ("**Base Agreement**"), as defined in point 1.1 of the General Terms and Conditions of Sale - Siemens, S.A., v. October 2023. The GTR shall also apply to Customer's indirect access to its own Systems via Remote Access.

2. Obligations of the Parties

2.1 Siemens shall setup the technical and organizational process for Remote Access and IT infrastructure used by Siemens for the establishment of the Remote Access according to Siemens security concept, as updated from time to time. Siemens is authorized to modify the Siemens' security scheme at any time without prior notice.

2.2 Siemens may provide Customer with information about the Remote Access status and general information on how to restore the connection in case it is not properly working.

2.3 The Customer shall, at its own cost and risk, provide the necessary interfaces and shall grant the necessary authorizations to enable Siemens to provide the Remote Services. Customer shall (i) maintain a state-of-the-art IT security scheme and infrastructure and (ii) ensure that the necessary security measures (e.g. system security updates, firewall setup and anti-virus programs) are taken and kept up-to-date at any time. Customer shall keep Siemens informed about its IT security processes and changes on the existing IT Security processes, systems and environment.

2.4 If the Remote Access cannot be used or is interrupted due to the Customer's security scheme, Siemens' obligation to perform the Remote Service shall be suspended for the duration of such interruption and without liability.

3. Access to Data

3.1 The Customer shall procure any and all rights, permissions and licenses for the Remote Access at its own cost and expense for the duration of the Basic Agreement.

3.2. Customer grants Siemens unrestricted access to Customer data to the extent necessary to provide the Remote Services.

3.3 While providing the Remote Services, Siemens may obtain, receive or collect data or information, including system-specific data or information or other content, from Customer and/or Customer System ("**Data**"). Customer hereby grants Siemens a non-exclusive, transferable, sublicensable, worldwide, royalty-free, perpetual, non-revocable license in all Data to provide the Remote Services

to Customer and to create derivative works and aggregated data derived from the Data, Siemens customers and other sources, including without limitation, comparative data sets, statistical analyses, reports and related services (collectively, "**Siemens Data**"). Siemens utilizes Siemens Data as it sees fit for any purpose.

3.4 Siemens may copy data from the Customer's Systems to its own systems if this is required to perform the Remote Services and/or the Basic Agreement.

3.5 Siemens must keep all Data it has received while performing the Remote Service separate from its other data and shall delete the same if and to the extent the data is no longer required for the performance of the Remote Service and/or Basic Agreement.

3.6 Siemens shall upon Customer's request within thirty (30) days, disclose the name of the staff members performing the Remote Service.

3.7 The data received from the Remote Service may be stored and processed outside the country of service. Such data may also be disclosed to Siemens AG, and/or any of its affiliates and/or consultants, in the course of performing the Remote Services and/or services under that Basic Agreement.

4. Access to personal data

4.1 Where Siemens requires access to personal data in order to perform the Remote Services, the Customer shall be informed and requested to authorize access. The personal data shall be accessed in accordance with the applicable law. The Customer shall abide by all data protection regulations and other legal and organizational rules and get all permissions required before granting access to personal data to Siemens. Siemens' obligation to provide the Remote Service shall be suspended without liability until approval is received.

5. Limited Warranty and Liability

5.1 The Remote Access is provided "as is" and Siemens does not provide Customer with any warranty or guarantee regarding the availability, performance or quality of the Remote Access other than explicitly agreed.

5.2 Siemens will not provide Remote Access if

- there is a defect, malfunction or other problem with the telecommunications network or
- there is a defect, malfunction, insufficient configuration or other problem with Customer's infrastructure

5.3 The limitation of liability of the Basic Agreement shall apply.

5.4 In the event of any loss of or damage to data and/or data storage media which occurs due to Siemens negligence Siemens's liability shall be limited to the costs for recovery of backed-up data. Any other liability of Siemens is excluded.

6. Termination

6.1 The Term for Remote Services shall correspond to the term of the Basic Agreement and/or as explicitly agreed.

6.2 Either party may suspend Remote Access with immediate effect if the Remote Access is misused or if risks for interruption or damage to the Customer System might occur. Where any such condition continues for longer than thirty days, these GTRs may be terminated by either Party.