Digital Services Supplemental Terms

Status: November 1, 2021

SIEMENS

These Digital Services Supplemental Terms ("**DS Terms**") amend the Universal Customer Agreement ("**UCA**") between Customer and Siemens solely with regard to Cloud Services. These DS Terms together with the UCA and other applicable Supplemental Terms form the agreement between the parties ("**Agreement**").

1. DEFINITIONS

Capitalized terms used herein have the meaning as defined elsewhere in the Agreement. The following additional definitions apply to these DS Terms:

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

"**Authorized Agent**" means an individual who requires access to the Offering in support of Customer's Permitted Use as consultant, agent, or in fulfillment of a contract with Customer, or who is otherwise expressly permitted in these DS Terms to access and use the Offering.

"**Authorized User**" or "**Named User**" means Customer's employee or Authorized Agent. Each Authorized User must use a unique user identification to access and use the Offering, unless a generic logon is expressly permitted in other Supplemental Terms, the Order or applicable Documentation. User identifications may not be shared with other individuals.

"**High Risk System**" means a device or system that requires 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 device or system could lead directly to death, personal injury, or catastrophic 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.

"Permitted Use" means Customer's internal use as end-user unless otherwise defined in other applicable Supplemental Terms or the Order.

"**Territory**" means the geographic area as specified in other applicable Supplemental Terms or the Order provided that Customer meets its obligations in the Agreement regarding compliance with export controls. If no geographic area is defined, the geographic area shall be the country, in which the Siemens entity named on the Order has its registered seat.

2. GENERAL

2.1 **Authorized Access and Use.** Each Offering may be accessed and used only by Authorized Users in the Territory for the Subscription Term, solely for the Permitted Use in accordance with the Entitlements and the Agreement. Customer may re-assign the right to access and use the Offering between uniquely identified individual Authorized Users over time, but not so frequently as to enable sharing by multiple Authorized Users. Indirect use of an Offering via hardware or software used by Customer does not reduce the number of Authorized User rights that Customer needs to acquire.

2.2 **Changes to Supplemental Terms. Enhancement of Offerings.** Siemens may only update these DS Terms and/or any other applicable Supplemental Terms during a Subscription Term, provided any such update does not (i) have a material adverse effect on Customer's rights (e.g. with respect to Entitlements or service levels) or (ii) result in a material degradation of the security measures maintained by Siemens with regard to the Offering or Customer Content. The foregoing shall not limit Siemens' ability to make changes to these DS Terms and/or any other applicable Supplemental Terms (i) to comply with applicable law, (ii) address a material security risk, (iii) to reflect changes made to the Offering in accordance with any change provision in the Agreement, or (iv) that are applicable to new features, supplements, enhancements, capabilities or additional Cloud Services or Software provided as part of Customer's subscription to the Offering at no extra charge. Any change to these DS Terms or any other applicable Supplemental Terms shall apply from the date as notified by Siemens or published on the website as referenced in the Order. Siemens will use commercially reasonable efforts to notify Customer at least 90 days prior to such change or as agreed elsewhere in the Agreement.

2.3 **Trial Updates.** Certain Offerings provide updates which will first be made available to Customer in a test instance for Customer's review prior to deploying a trial update in production ("Trial Update"). Siemens will give Customer notice when a Trial Update is first available and the date when the production environment of the Offering will be updated. Customer's entitlement to use any Trial Update in a test instance is limited as provided in the Agreement with the expectation that Customer will provide Feedback to mitigate any concerns when the production environment is subsequently updated. Updates to the production environment for Offering will occur on a fixed date for all Customers.

2.4 **High Risk Use.** Customer acknowledges and agrees that (i) 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 Offering and (ii) the outcome from any processing of data through the use of the 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 Offering for the operation of or within a High Risk System.

2.5 **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 Offering.

2.6 **Specific Terms for Remote Service**. Certain Offerings provide a means for secured remote login, remote engineering, or data transfer. Customer acknowledges that data traffic 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. It is Customer's responsibility to check if such local restrictions or prohibitions apply and to use Offerings in compliance with applicable law.

2.7 **Specific Terms for Content Sharing.** Certain Offerings enable Customer to grant a third party with authorized access to the Offering ("Receiving Party") access to certain Customer Content (read or read and write) under a collaboration ("Collaboration"). Once the Collaboration is established, the sharing party will be able to share selected Customer Content with the Receiving Party("Sharing"). Collaboration and individual Sharing require prior approval of the involved Receiving Party. It is expressly understood that the Collaboration is only between the Receiving Party and the sharing party and Siemens is not a party thereto, and the outcome of any Collaboration and Sharing of Customer Content is beyond Siemens' control. Customer is responsible for the implementation of measures required to reasonably protect Customer Content from misuse by any third party.

2.8 **Third Party Content.** Customer specifically acknowledges that (i) Siemens is under no obligation to test, validate, or otherwise review Third Party Content, (ii) Third Party Content may collect and use Customer Content and data regarding a User's usage of Third Party Content, and (iii) Customer is responsible for the development and technical operation of Customer Content, including compatibility of any calls Users make to Offerings.