Cybersecurity Conditions – Exports
Siemens Healthcare

Version: 1 October 2020

1 Scope and Definitions

1.1 Scope of these Conditions

These Conditions shall apply between the Customer and the contracting Siemens Healthineers entity ("Siemens Healthineers"). They are aimed at supplementing the General Conditions Supply and Delivery – Exports, Healthcare, if applicable, and shall prevail in case of conflict.

1.2 Definitions

"Product(s)" means products and solutions consisting of hardware and/or software which are sold, licensed or otherwise made available to the Customer by Siemens Healthineers, irrespective of whether the manufacturer is Siemens Healthineers or a third party. Provided however, that making available shall not include soliciting of respective transactions between the Customer and a third party, such as brokering third party Apps on the Siemens Healthineers Digital Ecosystem or other Siemens Healthineers platforms.

"SRS" means Smart Remote Services, i.e. an online connection between Siemens Healthineers and the relevant Product at the Customer's site allowing for remote distribution of software updates and Patches.

„IT Security" means safeguarding the uninterrupted operation of the Product(s) against interference caused by exploited Vulnerabilities as well as the availability, confidentiality and integrity of data and information.

"Cyberthreat" means any circumstance or event with the potential to adversely impact a Product via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

"Vulnerability" means a weakness in a Product that could be exploited by a Cyberthreat.

"Irrelevant" means a categorization of a Vulnerability the exploitation of which, taking into account the individual Product attributes and/or the respective operating environment, is not reasonably to be expected and/or would not result in a foreseeable impairment of the Product's secure operation.

"Patch" means a Software-Update with a fix for a Vulnerability.

"EoS" means End of Support, i.e. the date notified by Siemens Healthineers to the Customer after which service parts and any other services for the Product are no longer available, respectively a previous date so notified, after which the support for the software components of the Product terminates.

1.3 Subject Matter

These Conditions are aimed at providing a fair balance of Customer's cooperation duties and Siemens Healthineers' obligations as regards to appropriately handling Cyberthreats.

2 Siemens Healthineers' service offering until EoS

2.1 Save where mandated otherwise by mandatory applicable law, the following provisions shall apply:

2.1.1 If the provision of Patches has been agreed upon in writing Siemens Healthineers shall make available Patches as set forth herein below for the agreed term, otherwise until EoS or up to 10 years following Product delivery, whichever occurs first, provided that

(i) Siemens Healthineers becomes aware of a Vulnerability which Siemens Healthineers does not classify as Irrelevant;

(ii) the Customer's Product version is the most recent or at least the penultimate version at the given time as per Section 3.4 below, and

(iii) in case of third party software the third party software provider has issued the respective Patch to Siemens Healthineers; Siemens Healthineers shall not be responsible to ensure that the third party software provider issues or continues to issue Patches.

2.1.2 Patches shall be made available by Siemens Healthineers pursuant to Section 2.1.1 within reasonable time allowing Siemens Healthineers the required testing and validating, in case of third party software following their making available by Siemens Healthineers' licensors. Depending on the severity of the Vulnerability Siemens Healthineers may elect to provide the Patch at the time and as part of upcoming routine updates.

2.1.3 If the Product is capable for SRS and the Customer enables remote distribution of the Patches via SRS, or if Patches are made available for download via teamplay Fleet and the Customer has opened a teamplay Fleet account, no installation fee will become due. Otherwise, if the Patch needs to be installed on site by Siemens Healthineers, Siemens Healthineers may charge the Customer for the expenses resulting from the installation.

2.2 Under Maintenance Contract

2.2.1 For Products covered by a valid maintenance contract Section 2.1.1 through 2.1.2 shall apply accordingly.

2.2.2 In case of conflict, the terms of the maintenance contract shall prevail. However, installation of Patches by Siemens Healthineers is not included in the contract scope unless explicitly set forth in writing.

3 Customer's Cooperation Duties

3.1 In order to protect the Products against Cyberthreats, it is necessary that the Customer implements – and continuously maintains – a holistic, state-of-the-art security concept for its IT infrastructure, including regular Vulnerability scanning, provided however, that

(i) scanning or testing shall not be performed during clinical use;

(ii) the system configuration and/or IT Security controls of the Product must not be modified; and

(iii) if during the deployment of the Product Vulnerabilities are identified by the Customer, the Customer shall align with Siemens Healthineers regarding the severity of the Vulnerabilities taking into account the individual Product attributes and intended operating environment and shall not refuse acceptance of the Product, if Siemens Healthineers classifies the Vulnerability to be Irrelevant.

3.2 The Customer is responsible for preventing unauthorized access to the Products including but not limited to changing passwords and other protective settings from their default values to individual ones. The Products shall only be connected to an enterprise network or the internet if and to the extent such a connection is authorized by Siemens Healthineers in the instructions for use and only when appropriate security measures (e.g. firewalls, network client authentication and/or network segmentation) are in place.

3.3 USB-storage media and other removable storage devices shall only be connected to Products if and to the extent such connection is authorized by Siemens Healthineers in the instructions for use and only when the risk of a malware infection of the Product is minimized through malware scanners or other appropriate means.

3.4 The Products undergo continuous development to further improve their IT Security. Siemens Healthineers strongly recommends that Product updates are applied as soon as they are available and that the latest Product versions are used by the Customer. The latter might include the purchase of upgrades of hardware and software by the Customer. Use of Product versions that are no longer supported, and failure to apply the latest updates/upgrades may increase Customer's exposure to Cyberthreats.

3.5 Customer shall notify Siemens Healthineers without delay in case of suspected or actual cybersecurity incidents or Vulnerabilities of the Products. Disclosure of such information to third parties requires prior consent by Siemens Healthineers.

3.6 In the event that the Customer resells a Product, it shall inform Siemens Healthineers in writing of the name and address of the new owner and shall impose upon him a corresponding obligation in case of further resale.

3.7 If Siemens Healthineers provides Patches via SRS or for download via teamplay Fleet, the Customer shall always install the Patches within due time in accordance with the respective installation instructions given by Siemens Healthineers. Otherwise Customer shall allow the installation of the Patches pursuant to Section 2.1.3, 2nd sentence, irrespective of whether the Patch has been made available based on contract, law or on a voluntary basis.

3.8 In order to get access to the teamplay Fleet and to Patches made available for download the Customer shall register and maintain the registration with the teamplay Fleet for the term of Customer's Product usage.

4 Liability

4.1 Unless otherwise agreed in writing, any right of the Customer to claim damages resulting from or related to Cyberthreats, such as but not limited to loss of data, downtime, business interruption, lost profit, cost for Product reset and/or data reconstruction, regardless of the legal basis, but in particular resulting from any duty under the contract or as a result of any tortious act, is hereby excluded. In particular Siemens Healthineers assumes no liability whatsoever for damage caused by

(i) Customers' intrusive IT Security testing;

(ii) unauthorized, modification of the system configuration or IT Security controls of the Product;

(iii) the installation of Patches which are not authorized by Siemens Healthineers; or

(iv) the Customer delaying the self-installation of Patches made available by Siemens Healthineers via SRS or for download via teamplay Fleet.

4.2 This shall not apply insofar as liability is established on the basis of the following:

(i) intent;

(ii) gross negligence on the part of the owners, legal representatives or executives;

(iii) fraud;

(iv) failure to comply with a guarantee granted;

(v) negligent injury to life, limb or health; or

(vi) negligent breach of a fundamental condition of contract ("wesentliche Vertragspflichten")

on the part of Siemens Healthineers, or

(vii) according to mandatory Product Liability Law.

4.3 However, claims for damages arising from a breach of a fundamental condition of contract shall be limited to the foreseeable damage which is intrinsic to the contract, provided that no other of the above cases applies.

4.4 The above provisions do not imply a change in the burden of proof to the detriment of the Customer.

5 Exclusive Remedy

5.1 The foregoing obligations of Siemens Healthineers as set forth in Sections 2 and 4 shall be the exclusive remedy and in lieu of any other rights and remedies the Customer may have in relation to Cyberthreats and any damage suffered therefrom whether under contract, law or otherwise.

5.2 However, upon request Siemens Healthineers shall be prepared to provide assistance in the Product reset against reimbursement of cost plus reasonable profit.

6 Update of Terms and IT Security Concept

6.1 Siemens Healthineers reserves the right to modify these Cybersecurity Conditions to reflect technical progress, changes in law and further developments of Siemens Healthineers' offerings and other unforeseen circumstances.

6.2 Such modifications shall not unreasonably discriminate against the Customer.

6.3 Siemens Healthineers shall inform the Customer of changes in writing by giving a reasonable period of notice of at least 28 calendar days stating that the changes shall be deemed to have been accepted by the Customer, if no objection is raised within the aforesaid deadline. Upon expiration of the deadline the changes shall become valid, if no objection has been raised by the Customer before the expiration date.