INSIGHTS HUB SUPPLEMENTAL TERMS FOR ALPHANUMERIC CODE ‘MSPH-P’

Siemens Digital Industries Software

These Insights Hub Private Cloud Supplemental Terms (“**Insights Hub Private Terms**”) amend the Universal Customer Agreement (“**UCA**”) between Customer (also named “you”) and Siemens solely with regard to the Offerings which have been assigned the alphanumeric code ‘MSPH-P’ or where these Insights Hub Private Terms are otherwise referenced on the Order. These Insights Hub Private Terms, together with the UCA and other applicable Supplemental Terms, form the agreement between the parties (“**Agreement**”). The offerings governed by these Insights Hub Private Terms primarily consist of Software and technical operations. Please note that the Cloud Service Level Agreement (SLA) available at www.siemens.com/sw-terms/sla does not apply to Insights Hub Private Cloud offerings in its entirety (see chapter 5). And applicable services or related provisions are addressed within this document.

1. DEFINITIONS

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

“Account” means one or more web-based account(s), individually or collectively, enabling access to and use of certain Offerings through a unique URL assigned by Siemens.

“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

“Asset” means the logical representation of a thing which can be a machine or an automation system with a single or multiple automation unit(s) e.g. PLC or even a factory site. Assets are defined by using an Asset Type.

“Asset Instance” means a physical and/or logical device connected to your Account (e.g., a specific motor within a factory). Each Asset Instance belongs to an Asset Type.

“Asset Type” means a homogenous group of physical or logical Assets with common characteristics which are reflected in a template.

“Authorized Agent” means an individual who (i) requires access to the Offering in support of Customer’s or Customer Affiliate’s internal business as consultant, agent or contractor, or (ii) is otherwise expressly permitted in these Insights Hub Private Terms to access and use the Offering.

“Authorized User” or “Named User means Customer’s and its Affiliate’s employee or Authorized Agent. Each Authorized User must use a unique user identification to access and use the Offering, unless use of a generic login is expressly permitted in these Insights Hub Private Terms or applicable Documentation. User identifications may not be shared with other individuals.

“Customer Application(s)” means Customer Content and software that interoperates with Customer Instance as made available by Customer to Users. Any Customer Application must provide value to Users which is distinct from the Foundation. Customer Applications exclude Software, Documentation and Siemens IP. Customer Applications include Self-hosted Application.

“**Customer Environment**” means Customer’s or Customer’s provider’s cloud infrastructure and operating environment on which the Foundation is being operated as further set out in the Documentation.

“Customer Instance” means that the license is restricted to a single standalone deployment of the Foundation, which is operated on Customer’s Environment, but excluding Third Party Content.

“Developer Material” means Software and other proprietary material or information made available to Customer by or on behalf of Siemens in the course of Siemens’ provision of Developer Services.

“Developer Services” means Offerings that enable Customer to develop and test Customer Applications.

“DevOps Guide” or “Guides” means the DevOps Guide available as part of the Documentation.

“**Foundation**” means Software which encompasses Siemens’ proprietary cloud-based service foundation which includes the industrial Internet-of-Things-solution ‘Insights Hub’.

“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.

“Insights Hub Launchpad” means the following: after login to the Account, the Insights Hub Launchpad appears. Similar to a desktop on any common operating system (OS), the Insights Hub Launchpad facilitates starting various assigned Cloud Services or Customer Applications.

“Insights Hub Private Operations” means operating the Customer Instance by or on behalf of Siemens or as defined in the Documentation.
“Operator Services” means Offerings enabling Customer to deploy, operate, publish and/or provide Customer Applications.

“Self-hosted Application” means software that is hosted by Customer (or a third party authorized by Customer) in Customer’s own responsibility outside Customer’s Instance. This includes, but is not limited to, software that runs on mobile devices such as smartphones or tablet computers (sometimes also referred to as a “mobile native application” and described in more detail in the Documentation).

"Territory" means worldwide (subject to Customer's obligations in the Agreement regarding compliance with export controls) unless a geographic area is specified on the Order.

2. **GENERAL**

2.1 **Authorized Access and Use.** Each Offering may be accessed and used (and Software may be installed) during the Subscription Term only by Authorized Users in the Territory and solely in accordance with the Entitlements and this Agreement. Customer may re-assign the entitlement to access and use the Offering from one Authorized User to another Authorized User within the same entitlement category once per calendar month.

2.2 **Deployment and Operation.** The deployment and operation of Customer Instance licensed under these Insights Hub Private Terms in Customer's Environment is part of the Software Subscription for the entire Insights Hub Private Software Subscription Term. Any applicable Professional Services will be subject to separate legal terms set out in statement(s) of work. Insights Hub Private Operations are subject to the Supplemental Terms for Professional Services available at www.siemens.com/sw-terms/supplements. The following stipulations of the UCA shall apply accordingly to Insights Hub Private Offerings: Section 5.2 (Changes to Cloud Services), 5.3 (Use of Messaging Services), 5.4 (Out of Scope), 5.5 (Acceptable Use Policy; Indemnity.), 5.6 Ownership and Use of Customer Content, 5.7 (Protection of Customer Content).

2.3 **Changes to Supplemental Terms or Guides; Enhancement of Offerings.** Siemens may only update these Insights Hub Private Terms during a Subscription Term if 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 will not limit Siemens' ability to make changes to these Insights Hub Private Terms (i) to comply with applicable law, (ii) to address a material security risk, (iii) to reflect changes made to the Offering in accordance with any change provision in the Agreement, or (iv) which 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. When Customer uses any such new feature, supplement, enhancement, capability or Cloud Services or Software, the then-current Insights Hub Private Terms available at www.siemens.com/sw-terms/supplements will apply to such use. In all other cases, if an update to the Supplemental Terms during a Subscription Term applies to Customer, Siemens will use commercially reasonable efforts to notify Customer at least 90 days prior to such change or in accordance with the notice provisions stated elsewhere in the Agreement. Siemens may change the Guides from time to time; changes will become effective upon release of a new version. However, during a Subscription Term, Siemens may, upon Customer's request, defer the change effective date to the end of the applicable Subscription Term, but not by more than 6 months. In the event of a conflict or inconsistency between the Guides and these Insights Hub Private Terms, these Insights Hub Private Terms will prevail.

2.4 **Customer's Obligation.** Customer is responsible to provide Siemens with access to Customer's Environment at any time upon Siemens' request to enable Siemens to provide the Insights Hub Private Operations. Upon expiry or termination of the Subscription, Customer shall enable Siemens to de-install the Insights Hub Private Offerings immediately from Customer's Environment and Customer shall stop using the Insights Hub Private Offerings upon the effectiveness of such termination or expiry.

2.5 **Changes to APIs.** During a Subscription Term, Siemens may alter any customer-facing API that Customer is using. If any such alteration is material and in a backwards-incompatible fashion, Siemens will provide Customer at least 12 months' prior notice, except that this notice will not be required if it (i) would pose a security of intellectual property issue to Siemens or the Offering or (ii) would cause Siemens to violate legal requirements.

2.6 **Development and Provisioning of Customer Content**. Customer will not subject any Offering to, or upload Customer Content that is subject to, a license that, as a condition of use, access, and/or modification of such content, requires that Siemens or Siemens' business partners' software or services provided by Siemens (i) are disclosed or distributed in source code form, (ii) are licensed to recipients for the purpose of making derivative works, (iii) are licensed at no charge, (iv) are not used for commercial purposes, or (v) are otherwise encumbered in any manner. 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 the configuration, combination, or use of an Offering with any Customer Content, Third-Party Content or other third-party equipment, software or services used by any User in connection with Offerings.

2.7 **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 that (iii) Customer is responsible for the development and technical operation of Customer Content including compatibility of any calls Users make to Offerings.

2.8 **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 Offerings; and (ii) the outcome from any processing of data through the use of Offerings 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.

2.9 **Documentation**. The specifics of Offerings and Entitlements are described in the Documentation available at https://plm.sw.siemens.com/en-US/insights-hub/ which is incorporated herein by reference. Documentation includes information such as applicable limits or other attributes and metrics, prerequisites, or scaling factors for the pricing such as number of Assets, and additional third-party terms which prevail for third-party software, technology, data, and other materials, including open-source software licensed from third parties.

2.10 **Notices**. Notwithstanding Section 13.6 of the UCA, notices to Siemens shall be sent to contract.mindsphere.sisw@siemens.com.

3. **SPECIFIC TERMS**

3.1 **Specific Terms for Developer Services.** The following terms will apply to Customer's use of Developer Services:

3.1.1 Customer Obligations. Unless otherwise agreed in writing or expressly permitted in the Agreement, when using Developer Services, Customer will: (i)use Developer Services solely for the development, testing, and demonstration of Customer Applications, but not for productive or other commercial use, (ii)ensure that Customer Applications comply with any applicable Guides or Documentation, (iii)not use any device, location, database, or application outside Customer Instance to enable transfer of any of Customer Content to a destination outside Customer Instance, and (iv)not allow any application, services, or other software deployed outside Customer Instance to interoperate with Foundation APIs, except to the extent required for the intended purpose of the applicable Offerings. Customer acknowledges and agrees that Developer Services are not designed to be used to access, use, or otherwise process any data that would qualify as Confidential Information.

3.1.2 Submission. Customer is responsible for (i)the evaluation and testing of each Customer Application as to its technology, functionality, performance, security, and user interface; (ii)the compliance of each Customer Application with the DevOops Guide and any other requirements set out in the Agreement; and (iii)the successful completion of any technical self-certification process made available by Siemens.

3.1.3 Review. Siemens reserves the right to review each Customer Application, whether directly or through a subcontractor, but is not obligated to conduct any such review. Neither any such review nor the lack thereof will constitute or be communicated by Customer to be an endorsement by Siemens of Customer Applications. Additional terms regarding review standards and processes may be set out in the DevOps Guide. Customer agrees to cooperate with Siemens in the review process and provide information and materials reasonably requested by Siemens, including information on the operation of Customer's business. Siemens may adopt and change its review standards or processes at any time as it deems appropriate. Any of Customer's non-public information that Siemens obtains access to in the course of the review will be considered Customer's Confidential Information.

3.1.4 Rejection. Siemens may reject the productive use of a Customer Application if Siemens determines that Customer Application (i) does not meet all or any part of the imposed requirements or (ii) might impact the proper functionality of Customer Instance and/or Siemens' Insights Hub Private Operations (e.g. due to cybersecurity threads, coding issues etc.). If Siemens rejects a Customer Application, such Customer Application will not be deployed on Customer Instance.

3.1.5 Rights in Customer Applications. Customer will own all intellectual property rights in, or to, Customer Applications and other results developed by or on behalf of Customer using the Developer Services, subject, however, to any rights of Siemens, rights of third parties, and rights in Developer Material.

3.1.6 License Grant. Siemens grants Customer a non-transferable, non-sublicensable, time-limited, and revocable license to use and permit third parties to use Developer Material solely for development and testing of Customer Applications.

3.2 **Specific Terms for Operator Services.** The following terms will apply to Customer's use of Operator Services:

3.2.1 Customer's Obligations. Unless otherwise agreed in writing or expressly permitted in the Agreement, when using Operator Services Customer will: (i) use Operator Services solely to deploy, operate, or provide Customer Applications for its own use; (ii) not develop or modify Customer Applications; (iii) ensure that Customer Applications comply with the DevOps Guide and any other requirements set out in the Agreement ("**Requirements**"); (iv)not use any device, location, database, or application outside Customer Instance to enable transfer of any Customer Content to a destination outside Customer Instance; and (v)not allow any application, services, or other software deployed outside the Customer Instance to interoperate with Insights Hub APIs, except to the extent required for the intended purpose of the applicable Offerings.

3.2.2 Maintenance and Removal. Customer will ensure that Customer Applications are kept up to date with current bug fixes and patches. If Siemens determines that Customer Applications do not meet the Requirements, Siemens may provide notice requesting that Customer update Customer Applications, so they comply with the Requirements. If Customer fails to remedy the non-compliance within the time period stated in the notice, Siemens reserves the right to remove such non-complying Customer Applications.

3.2.3 Support; User Documentation. Customer is responsible for providing support concerning Customer Applications. Customer will provide user documentation that accurately reflects the functionalities of Customer Applications, including security safeguards and information explaining which functionality resides outside Customer Instance.

3.3 **Specific Terms for Data Sharing**. Certain Offerings enable Customer to grant another Account access to certain Customer Content (read or read and write) under a collaboration ("**Collaboration**"). Once the Collaboration is established, the sharing Account will be able to share selected Customer Content with the receiving Account ("**Sharing**"). Collaboration and individual Sharing require prior approval of the involved Accounts. Between Siemens and the involved Accounts, it is expressly understood that the Collaboration is only between the involved Accounts 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.

3.4 **Specific Terms for Self-Hosted Applications.** Certain Offerings enable Customer to register a Self-hosted Application to its Account in order to deploy, operate and provide it to Customer. Customer is solely responsible for procuring and maintaining appropriate licenses for all third party software or services that Customer uses in relation to its Self-hosted Application (including for the hosting and operation thereof).

3.5 **Specific Terms for MindConnect Device Management Services.** By using MindConnect Device Management Services, Customer acknowledges and agrees that (without limiting any of Customer's further obligations under the Agreement) (i) any transfer and deployment of configuration files, firmware images, or other data or software, as well as corresponding documentation or terms and conditions to connected devices is solely agreed between Customer and the relevant device owner/user, and (ii) Siemens does not assume any obligations or responsibility with regard to, and is under no obligation to test, validate, or otherwise review, such content.

4. INSIGHTS HUB PRIVATE OPERATIONS

4.1 General

4.1.1 Updates. We may make updates to this section 4 to improve the operations activities. The then-current section 4 will apply to the provisions of the operations activities to you.

4.1.2 Remote Services. All services shall be provided remotely in English language.

4.1.3 Your Responsibilities. This section outlines your responsibilities which are in addition to those responsibilities outlined in the Agreement which governs this Section 4.

a. General

i. You will provide us with all the information regarding your business, equipment, work procedures and plans which are required by us to render the deliverables and will ensure that any information provided is accurate and complete.

ii. You coordinate monthly meetings with us and other relevant stakeholders for deployment alignment and planning.

iii. Your operating environment meets all the prerequisites as described in Section 4.4 so that we may carry out the activities described in this Section 4. The availability of a qualified infrastructure is a critical success factor for the timely execution of the activities with the expected level of quality.

iv. You shall provide Insights Hub Private Cloud Software subscription as needed for your purposes.

v. You shall be solely responsible to contract for telecommunications facilities (data communications circuit, wiring, etc.), and for the costs associated with such facilities.

vi. You shall be responsible for implementing and maintaining your information security controls for internet service provisioning according to ISO 27001 or equivalent.

vii. You shall adequately plan your infrastructure to accommodate number of Users to access your Insights Hub Private instance.

b. Insights Hub Cloud Dedicated (Virtual Private Cloud)

i. You shall provide the Infrastructure as a Service ("IaaS") subscriptions as described in Section 4.4.

ii. We receive all administrative permissions (here: administrator privileges) to the IaaS subscriptions provided by you.

iii. You coordinate between us, the IaaS supplier and other relevant third parties to provide all required information to us in a consolidated form.

c. Insights Hub for Private Cloud (Local Private Cloud)

i. You shall provide third party and open-source software and respective licenses and operate your operating environment as laid out in Section 4.4.

ii. You coordinate between us and relevant third parties to provide all required information to us in a consolidated form.

iii. You will be responsible for the infrastructure and network maintenance per the specification provided by Siemens.

4.1.4 Out-of-Scope Responsibilities for Us. The following non-exhaustive list shows examples of activities not in the Insights Hub Private Operations' scope:

a. Any data upload services or tools to migrate or clean legacy or supplier/partner data into or out of your Insights Hub instance. You are responsible for data migration.

b. All activities, which are not explicitly mentioned in this Section 4, e.g. training, data backup and recovery procedures, certificates, monitoring, Review of your information security controls.

c. Third party applications on your Insights Hub instance.

d. Reviewing your information security controls.

4.1.5 Your Project Manager or Single Point of Contact (Recommended). You will provide a project manager to act as your representative to us. This project manager will be responsible to:

a. Provide required information relevant to accomplishing the work activities quickly and accurately.

b. Provide your organizational linkages, including the appropriate people and teams.

c. Ensure availability of key business subject matter experts on a best-effort basis during designated meetings, with the proper level of decision-making.

d. Provide your input, assistance, participation, and cooperation with our activities and requests required by the in-scope activities tasks of this Section 4.

e. Provide us with all your management decisions and responses, information, data, equipment, approvals if any in a timely manner.

f. Provide your business processes to us.

4.2 Initial Deployment

4.2.1 Kick-Off. For the detailed planning of the deployment preparation, we shall prepare, perform, and document a remote kick-off meeting with you.

4.2.2 Readiness of Operating Environment. We shall verify if you are meeting all Insights Hub private install and system management prerequisites as described in Section 4.4 for your operating environment, such as e.g., proper sizing of the systems, system access, or installed software versions. We shall prescribe the required system updates to be implemented by you as necessary. We shall confirm when your operating environment meets all Insights Hub installation and system management prerequisites and declare its readiness for the initial deployment of the Insights Hub Private Software. Implementation of system updates necessary to fulfill the prerequisites for the readiness of the operating environment are not executed by us.

4.2.3 Readiness of Hardware. Readiness of the hardware will be validated by Siemens operations team for Insights Hub Local Private Cloud deployment. Hardware specification will be given by Siemens operations team based on the load profile to be supported in the customer environment. Customer or partners is supposed to arrange the hardware based on specification and before IH deployment siemens operations team is going to validate the initial configuration.

For Insights Hub Virtual Private Cloud deployments, this is not applicable, as the Siemens operations team will manage the entire infrastructure deployment.

4.2.4 Initial Deployment. We shall align with you on a timeline for performance of the initial deployment. Provided that the operating environment is ready, we shall deploy the Insights Hub Private Software on your operating environment per remote installation according to the agreed timeline.

4.2.5 Completion of Deployment and Access Credentials. Upon completion of the initial deployment of the Insights Hub Private Cloud Software on your operating environment, we shall announce the completion to you and provide you with the access credentials to your Account.

4.3 Insights Hub Private Operations

4.3.1 Content of Insights Hub Private Operations. We shall operate the Insights Hub Private Cloud Software as described in this section, hosted on an operating environment provided by you and dependent on the fulfillment of further obligations by you, and thus make the Insights Hub instance available to you. Management of your operating environment is not included in the Insights Hub Private Operations.

4.3.2 Insights Hub Cloud Dedicated (Virtual Private Cloud). With regards to Insights Hub, the operations consist of the following actions:

a. Environment Access

Action	Customer	Siemens
Lifecycle management of user access to IaaS accounts	Yes	
Lifecycle management of technical access to IaaS accounts	Yes	Yes

To perform operational duties, access to the IaaS accounts shall be managed by you and continuously ensured for us.

Technical access to the IaaS API is granted by you by ensuring a trust relationship with a Siemens managed vault instance.

Network access to your Insights Hub instance is coordinated between you and us.

All the accesses above must be available for our operational support.

b. Deployments

Action	Customer	Siemens
Coordination of deployment windows	Yes	Yes
Deployment of Insights Hub Private Cloud Software component updates/patches and configuration of required IaaS services		Yes

You shall define a responsible contact person to coordinate deployments of Insights Hub Private Cloud Software components. Time slots for deployments should be set in regularly scheduled meetings.

c. Monitoring

Action	Customer	Siemens
Monitoring setup to review health of Insights Hub Private Cloud Software components installed in your infrastructure (e.g. IaaS accounts) by us	Yes	Yes
Live monitoring of alerts	Yes	

We continuously monitor the health of installed Insights Hub Private Cloud Software components. To this purpose health metrics will be exported into our central monitoring service.

d. Configuration

Action	Customer	Siemens
Environment for your Insights Hub instance configuration coordination	Yes	Yes
Changes to configuration of environment for your Insights Hub instance		Yes

Both parties shall coordinate a suitable environment configuration. This should be reviewed by both parties on a regular basis and adjusted to demands (e.g., for scaling).

Any changes to the environment configuration of your Insights Hub instance shall be implemented by us.

e. Incident Management

Action	Customer	Siemens
Automatic detection of predefined Insights Hub Private Cloud Software system alerts	Yes	
Manual reporting of incidents via Support Center	Yes	
Response to automatically/manually reported outages		Yes
Incident documentation		Yes
Emergency deployment decisions		Yes
Root cause analysis on outages	Yes	Yes
Receival and forwarding of incidents reported by your IaaS supplier	Yes	

We will leverage continuous health monitoring to automatically detect Insights Hub Private Cloud Software system alerts indicating non availabilities. Incidents reported in this manner or manually by you via the Support Center will be responded to by us and we will directly access your Insights Hub instance to stabilize the system.

To be able to respond in time, we shall be able to unilaterally decide to deploy changes for the purpose of incident remedy.

For the purpose of minimizing outage occurrences, each instance shall result in us performing and documenting the root cause. You shall support this effort.

Incidents reported by your IaaS supplier shall be forwarded to us by you for further processing.

4.3.3 Insights Hub for Private Cloud (Local Private Cloud). With regards to Insights Hub, the operations consist of the following actions:

a. Environment Access

Action	Customer	Siemens
Admin access to infrastructure accounts	Yes	Yes
Admin access to your environment	Yes	Yes

Network access to your environment is coordinated between you and us.

All the accesses above must be available for our operational support.

b. Deployments

Action	Customer	Siemens
Coordination of deployment windows	Yes	Yes
Cluster and Backend services	Yes	
Deployment of Insights Hub Private Cloud Software component updates/patches and configuration of required operating environment		Yes

You shall define a responsible contact person to coordinate deployments of Insights Hub Private Cloud Software components. Time slots for deployments should be set in regularly scheduled meetings.

c. Monitoring

Action	Customer	Siemens
Monitoring setup to review health of Insights Hub Private Cloud Software components installed in your operating environment	Yes	Yes
Monitoring setup to review health of Cluster and Backend Services	Yes	
Live monitoring of alerts	Yes	

We continuously monitor the health of installed Insights Hub Private Cloud Software components. To this purpose health metrics will be exported into our central monitoring service.

d. Configuration

Action	Customer	Siemens
Environment for your Insights Hub instance configuration coordination	Yes	Yes
Changes to configuration of environment for your Insights Hub instance		Yes

Both parties shall coordinate a suitable environment configuration. This should be reviewed by both parties on a regular basis and adjusted to demands (e.g., for scaling).

Any changes to the environment configuration of your Insights Hub instance shall be implemented by us.

e. Incident Management

Action	Customer	Siemens
Automatic detection of predefined Insights Hub Private Cloud Software system alerts	Yes	
Manual reporting of incidents via Support Center	Yes	
Response to automatically/manually reported outages		Yes
Incident documentation		Yes
Emergency deployment decisions		Yes
Root cause analysis on outages	Yes	Yes

We will leverage continuous health monitoring to automatically detect Insights Hub Private Cloud Software system alerts indicating non availabilities. Incidents reported in this manner or manually by you via the Support Center will be responded to by us and we will directly access your Insights Hub instance to stabilize the system.

To be able to respond in time, we shall be able to unilaterally decide to deploy changes for the purpose of incident remedy.

For the purpose of minimizing outage occurrences, each instance shall result in us performing and documenting the root cause. You shall support this effort.

4.4 **Operating Environment Prerequisites**

4.4.1 Insights Hub Cloud Dedicated (Virtual Private Cloud). The following prerequisites apply to you when using IaaS from AWS or Microsoft Azure as your operating environment.

Requirements	Details
Subscriptions	1 IaaS subscription

Backing Services	Part of your IaaS subscription.
DNS	Will require below 3 delegated DNS and CA certificates associated with this: • *.xiot.<customerbasedomain> • *.piam.xiot.<customerbasedomain> • *.uiam.xiot.<customerbasedomain>
SSL	Based on SAN. You will provide SSL certificates to us for the installation.
ADFS	Your IDP information should be provided to us for the integration so that we will be able to access your environment.
SMTP Server	You should provide the SMTP server details to integrate with Insights Hub notification services for email notifications.

4.4.2 Insights Hub for Private Cloud (Local Private Cloud). The following prerequisites apply to you when using an operating environment other than IaaS.

a. General Prerequisites on your operating environment

Requirements	**Details**
ADFS	Your IDP information should be provided to us for the integration so that we will be able to access your environment.
Backing Services	All backing services should be deployed by you with Insights Hub specified configurations and namespace and ready for the Insights Hub Private Cloud Software installation. Please see the Backing Services section below for details.
Deployment Environment	Availability of operating environment according to Insights Hub specific configuration, with following specifications: • Admin access will be provided to us. • Ingress setup is complete with wildcard and ingress logs are enabled.
DNS	*.xiot.<customerdomain>, *.piam.xiot.<customerdomain>, *.uiam.xiot.<customerdomain>, *.apps.<cluster-name>.<customerdomain>, api.<cluster name>.<customerdomain> These domains need to be added to your DNS server.
Monitoring prerequisites	• Monitoring metrics data source to be exposed to Siemens network. • Alerting channel (PagerDuty, Slack, Teams, Webhook, Mail, etc.) needs to be provided by you for the incident alert.
SMTP Server	You should provide the SMTP server details to integrate with Insights Hub Notification services for email notifications.
SSL (for external communication)	• *.xiot.<customerdomain>, *.piam.xiot.<customerdomain>, *.uiam.xiot.<customerdomain> the certificate is needed for your Insights Hub Private instance. • *.apps.<cluster name>.<customerdomain>, api.<cluster name>.<customerdomain>: the certificate is needed for your operating environment.

Static virtual IP	Two static IP associated with below DNS entries need to be configured to your DNS server. • IP1 - *.apps.<cluster name>.<customerdomain> • IP2 - api.<cluster name>.<customerdomain>

b. Deployment Environment

i. OpenShift/Rancher: The compatible versions for the deployment environment are listed at https://documentation.mindsphere.io/resources/private-cloud/Backing-Services.pdf.

ii. Hardware Requirements: to be aligned project specifically between you and us.

c. Backing Services: The compatible versions for the operating environment are listed at https://documentation.mindsphere.io/resources/private-cloud/Backing-Services.pdf.

5. **SUPPORT**

For detailed information regarding Technical Support, please refer to Chapter 2 of the Cloud Service Level Agreement (SLA), available at www.siemens.com/sw-terms/sla. Siemens offers technical support and service levels in tier "Standard" only.