Terms of Use for the
Inuatek Data Collection Cloud (DCC)

(Hereinafter the "TOU" or "this Agreement")

Version 2.4 2024

Inuatek A/S ("Supplier")
Refshalevej 163A
1432 Copenhagen K
Denmark
VAT no.: DK-40051244

1 About Supplier and Terms

1.1 The “Terms” for the Data Collection Cloud (Hereinafter the DCC) consists of a specific order confirmation or agreement, the “General Terms and Conditions” agreement (Accepted by the company having entered the commercial agreement with Supplier for the DCC, hereinafter the GTC) and the “Terms of Use” agreement (This agreement presented to a User at first login or when changed, hereinafter the TOU or this Agreement), which collectively regulate the use of a Supplier hosted version of the DCC. This includes any white-labelled version, including but not limited to ADM4.0. All versions are in the following referred to as DCC.

1.2 The DCC is produced and marketed by Inuatek A/S, a Danish Private Limited Company registered under the Central Business Registration (in Danish: “CVR”) No. 40051244 (hereinafter “Supplier”).

1.3 The User (in singular or plural) mentioned throughout this Agreement shall mean the user of the DCC, both as a regular user or as an administrator. The term Customer is used in relation to the commercial agreement with Supplier for the DCC. User and Customer may represent the same or separate individual or legal entity respectively.

1.4 This Agreement shall be considered accepted by the User/Customer by agreeing to these terms at User first time login to the DCC, and when this Agreement is updated.

2 Supplier Hosted DCC vs Customer Hosted DCC

2.1 The following paragraphs refer to Supplier Hosted DCC. If the DCC you login to is not hosted by Supplier, different terms may apply. In this case refer to your point of contact about applicable terms.

3 Supplier Hosted DCC - Unauthorized use of the DCC

3.1 Unauthorized use of DCC includes any use that may compromise security, stability, Internet etiquette, legal regulations, or any operation that interferes with or disrupts the integrity or performance of DCC, including but not limited to:

3.1.1 Penetration testing on the DCC other than by agreement with Supplier;

3.1.2 Attempting to interfere in any way with the DCC, our hosting services, our website, or our network security, or attempting to use the DCC, our hosting services or our website to gain unauthorized access to any other computer system;

3.1.3 Using the DCC for distribution of malware or other malicious data that may cause damage to Supplier, Customer or third-parties;

3.1.4 Reverse engineering, decompiling or otherwise attempting to reconstruct or discover any source code or underlying ideas or algorithms of the DCC and hosting services (unless explicitly allowed by us or applicable law);

3.1.5 Use of the DCC for any illegal or fraudulent activities, including but not limited to hacking, phishing, identity theft, and copyright infringement;

3.1.6 Use of the DCC for sending spam or engage in any other form of unsolicited communication or marketing;

3.1.7 Use the DCC or the hosting services to conduct any activity that may violate the laws of your country or region;

3.1.8 Other harm to Supplier or Customer in any other way, determined at our sole discretion.

3.2 Supplier reserves the right to monitor the use of the DCC including the content on specific web sites to interrupt and prevent any unauthorized use.

3.3 Supplier shall have the right, without being liable towards the User, to shut down access to the DCC without prior warning if a User makes unauthorized use of DCC.

3.4 If Supplier shuts down the access due to unauthorized use, Supplier shall immediately after the shutdown inform the User in writing of the shutdown and the reason therefore.

3.5 Once the User has ensured Supplier that unauthorized use will not happen again the User's access may be reopened against payment of a handling fee to Customer.

3.6 The User shall indemnify and hold Supplier harmless against any and all costs and losses incurred as a consequence of the User's unauthorized use of the DCC.

4 Supplier Hosted DCC - Privacy Policy

4.1 Account Isolation and Access:

4.1.1 Company accounts on the DCC are isolated from each other. Only authorized and trusted employees of Supplier have access to these accounts for maintenance and support purposes.

4.1.2 Access to or modification of IoT Device configurations by Supplier employees will occur only with explicit consent provided by an authorized representative of the User's company account.

4.2 Device Ownership and Reassignment:

4.2.1 Supplier may, upon receiving adequate proof of IoT Device ownership and clear instructions from the owner, release the binding of an IoT Device from the current User's company account.

4.2.2 This process will result in the deletion of all configurations, event histories, and collected data associated with the IoT Device.

4.3 Account Creation and Access:

4.3.1 Supplier will only assist in creating the initial Administrator account for a company. Supplier employees will not facilitate account access or linkages between separate company accounts.

4.4 GDPR Compliance Overview:

4.4.1 The DCC is operated in compliance with GDPR requirements applicable to organizations processing the personal data of EU residents.

4.4.2 The DCC infrastructure is hosted within the EU region.

4.4.3 The personal data stored about Users includes only the name, email, and optionally, a mobile phone number. This information is secure based on the DCC's mechanism for encryption of data "at rest".

4.5 Data Processing and Usage:

4.5.1 Supplier acts as a Data Processor for the personal data contained in the User's account and any additional User accounts created under the User's administration.

4.5.2 User account information is used exclusively for communication relevant to the operation of Supplier products and services. This includes service messages related to maintenance, security, and product updates. Any promotional or non-operational communication will require User's explicit consent and is not covered under this agreement.

4.5.3 If the DCC is operated by a Distributor on behalf of the Supplier, the Distributor is contractually obligated to process personal data only for the purposes described herein.

4.6 Backup and Restoration:

4.6.1 Backup data is maintained solely for the purpose of restoring services in the event of system maintenance or failure.

4.7 Responsibility for Additional Users:

4.7.1 If the User account permits the creation of additional user accounts for others, including employees or external collaborators, The User and the User's company bear full responsibility for ensuring GDPR compliance concerning these individuals.

4.8 Monitoring and Validation

4.8.1 Supplier may monitor Users use of the DCC to ensure compliance with this Agreement and protect the integrity of the system. This monitoring is limited to what is necessary to fulfill these purposes.

4.9 Responsibility for Collected Personal Data

4.9.1 IoT Devices connected to the DCC are used to collect personal data, User's company is solely responsible for ensuring GDPR compliance for such data, whether stored within or transmitted through the DCC.

5 Supplier Hosted DCC - Support

5.1 Unless otherwise agreed between Supplier and Customer, the User has free email/web support all working days from the point of purchase (Supplier or Supplier's Distributor if purchased via such). Support does not include specific implementation or system design assistance, which may be subject to normal consultancy terms. Note that terms of support may vary between Supplier and Distributors.

5.2 The features available to a User may be limited by the User account type or the agreement entered between the Supplier/Distributor and Customer. Refer to your point of contact to determine whether limitations to your account apply. Supplier will not engage in changing your account type or granting access to certain features unless explicitly instructed by the Customer.

5.3 For Users purchasing directly from Supplier the following apply:

5.3.1 Supplier provides support between 09:00 a.m. and 4:00 p.m. CET/CEST and are closed on national holidays. Supplier global affiliates may have different opening hours.

5.3.2 Inquiries must be sent to support@inuatek.com or via the Contact form on www.inuatek.com and must clearly state the purpose and User's contact details. If the inquiry is about technical support, the User should describe the problem,

expected behavior, and the specific IoT device and names of other functions involved, such as report, even trigger, dashboard etc.

5.3.3 Supplier will reply to inquiries on a “first come, first served” basis. The response time usually never exceeds twenty-four (24) hours during Danish working days.

5.3.4 If Customer has signed a separate prioritized support or maintenance agreement with Supplier, appointed Users should report requests at the Supplier service desk, currently https://inuatek.atlassian.net/servicedesk/, or by a phone number provided to the User. Note that the User must have an account on the Supplier service desk.

5.3.5 Support from Supplier will be provided by English speaking support employees.

6 Supplier Hosted DCC - Trial mode

6.1 In case User is using the DCC in Trial mode, the following additional conditions apply, unless any other agreement is made between Supplier and Customer:

6.1.1 A newly connected IoT Device can operate free of charge for a period of 30 days (This period may vary for different white label versions of the DCC). The trial period can be used for testing as well as production purposes. The IoT Device will not stop collecting data after trial expiry, which will give Customer time to enter a paid plan without losing historic data.

6.1.2 If Customer has not chosen to enter a paid plan, the account, IoT Devices and collected data may be deleted at any time.

7 IoT Device Installation and configuration

7.1 Any installation of an IoT Device connecting to the DCC is contingent upon the User providing the following at User's own cost and effort:

7.1.1 Adequate Internet access.

7.1.2 Adequate knowledge about setup and configuration of the IoT Device.

7.1.3 Adequate knowledge of Data formats of the relevant Industrial Equipment to collect Data from.

7.1.4 Adequate authority to apply the IoT Device to the Industrial installation and allow Collection of Data.

7.2 The User shall prior to installing the IoT Device ensure that the Industrial Equipment in question is enabled for data collection access by a protocol supported by the IoT Device.

7.3 Supplier is not liable for data transmission to and from the Industrial Equipment, as Supplier has no control over the internet or the User's internal IT installations. Nor is Supplier liable for the correctness of data received.

7.4 The User has been made aware that data between the Industrial Equipment and the IoT Device may be transferred in a non-encrypted format.

7.5 The User has been made aware that all data between IoT Device and DCC is encrypted.

----oooOooo---