CONNECTED SOLUTIONS - END USER AGREEMENT

This end user agreement (the "**Agreement**") is a legal agreement between you, an individual or entity, ("**you**" or "**your**") and either: (i) Honeywell International Inc. ("**HII**"); or (ii) if there is a Company Agreement (as defined below) and HII is not a party to it, each HII affiliate(s) that is a party to the Company Agreement ("**us**", "**we**" or "**our**") regarding your: (i) use of software and/or applications provided to you by us or our affiliates ("**Honeywell**"), either directly or indirectly including via resellers or on-line store (the "**Software**"); and/or (ii) access to online portals, internet sites and other interfaces or means of access to our products and services including VPNs, APIs etc. ("**Portals**"). If you are using the Software or Portals on behalf of, or given access by, your employer or another entity (the "**Company**"), this Agreement may be supplemented by separate terms and conditions executed between Company or related entities and us or our affiliates relating to the Software or Portals (the "**Company Agreement**") and this Agreement will not be construed to limit any rights, obligations or responsibilities in any such agreement.

By downloading or installing the Software or accessing the Portals and/or clicking "Agree" (or similar term) you are agreeing to and representing the following on behalf of yourself and any other entities or persons whose data is being provided as Input Data, (as defined below) ("**Relevant Parties**"):

- You have authority to enter into this Agreement on behalf of your employer and any Relevant Parties and agree to be bound by its terms. If you do not have authority to enter into this agreement or do not agree to the terms of this Agreement, do not click "ACCEPT" or use the Software or Portal;
- You have sole responsibility for obtaining all consents and permissions including providing notices to users of the Connected Solution (each a "**User**") or third parties and satisfying all requirements necessary to permit our use of Input Data or Personal Data (as defined below) as set out in this Agreement.
- Any contact information and other information you provide to us is accurate and complete, including, but not limited to, any email addresses or other contact information, and that we may use such information for the use and purposes contemplated herein.

1. **Rights**. Subject to payment of applicable fees and Clause 2 and for the period you are authorized by us to access the Software or Portals we: (i) hereby grant you a personal, revocable, non-exclusive, non-assignable, non-transferable right to download, install, and use a single copy of the Software and any related documentation, solely for your own business or other permitted purposes; and (ii) shall provide you access to Portals we provide to execute the features and functions of our products and services. You may not resell the Software or Portals or, permit third parties (except affiliates) to use them or make copies (except for back up purposes) unless agreed by us in writing. We reserve all of our intellectual property rights in the Software and Portals including any not expressly granted to you in this Agreement.

2. **Acceptable Use.** You shall not use the Software or Portals for purposes of, or in connection with: (a) reverse engineering, making machine code human readable or creating derivative works or improvements; (b) introducing, transmitting or storing malicious code; (c) interfering with their security or operation; (d) framing or mirroring outside of your own intranets; (e) creating, benchmarking or gathering intelligence for a competitive offering; (f) defaming or harassing, transmitting obscene, libelous or otherwise unlawful materials; (g) infringing another's intellectual property rights including failing to obtain permission to upload/transfer/display works of authorship; (h) intercepting or expropriating data; (i) spamming, spoofing or otherwise misrepresenting transmission sources; (j) probing, scanning or testing the vulnerability of any security measures associated with the Software or Portals or supporting system or network; (k) employing them in hazardous environments requiring fail-safe performance where failure could lead directly or indirectly to personal injury (including death) or property or environmental damage, such as nuclear facilities, aircraft navigation or communication, traffic control, direct life support or weapons systems; or (l) any use that would reasonably be expected to cause liability or harm to Honeywell or our customers. During the term of this Agreement and 24 months after, we or our designee can, during normal business hours upon reasonable notice, access, inspect and audit, your compliance with this Agreement and you will furnish such information and access to personnel as we may reasonably request. We have the right to monitor usage. You shall not remove, modify or obscure any proprietary rights notices.

3. **Accounts, Updates, Support**. In operating your account you must; (i) maintain strict confidentiality of User names, passwords or other credentials; (ii) not allow others to use your credentials or access your account; and (iii) immediately notify us of any unauthorized use or breach of security related to your account. You will be responsible for access by any party you authorize. We may use rights management features (e.g. a lockout) to prevent unauthorized use. We or an applicable app store may automatically install updates to any Software or Portal. If you do not want to have updates installed, your remedy is to stop using the Software or Portal. If you are provided with an option to update, you understand that failure to do so may mean loss of features or functions including security. We are not providing you with any dedicated support or maintenance for the Software or Portal, except to the extent agreed otherwise in writing (including in any relevant Company Agreement). We are not responsible or liable for any problems, unavailability, delay or security incidents arising from or related to: (i) conditions or events reasonably outside of our control; (ii) cyberattack; (iii) the public internet and communications networks; (iv) data, software, hardware, telecommunications, infrastructure or networking equipment not provided by us; (v) your and Users' negligence or failure to use the latest version or follow published documentation; (vi) modifications or alterations not made by us; or (v) unauthorized access via your credentials.

4. **Data**. As between us and you and unless agreed otherwise in any Company Agreement, you retain all rights over data and other information that you or persons acting on your behalf input, upload, transfer or make available in relation to, or which is collected from your devices or equipment by, the Software or Portals ("**Input Data**"). Unless agreed otherwise in the Company Agreement: (i) Honeywell has the right to retain, transfer, disclose, duplicate, analyze, modify and otherwise use Input Data to provide, protect, improve or develop our products or services; and (ii) Honeywell may also use Input Data for any other purpose provided it is in an anonymized form that does not identify you. All information, analysis, insights, inventions and algorithms derived from Input Data by Honeywell or its affiliates (but excluding the Input Data itself) and any intellectual property rights obtained related thereto, are owned exclusively and solely by us and are our confidential information. Any Personal Data contained within Input Data shall only be used or processed in accordance with Clause 5, the data privacy terms of any relevant Company Agreement and applicable law. You have sole responsibility for obtaining all consents and permissions (including providing notices to Users or third parties) and satisfying all requirements necessary to permit our use of Input Data.

5. **Privacy.** Honeywell may process personal data about individuals (e.g. about you, Users and/or other employees, contractors and/or agents of your Company or its affiliates) that is recognized under applicable privacy laws as "personal data" or equivalent terms (collectively, **"Personal Data**") in relation to the performance of this Agreement or Company Agreement and the provision of the Software or Portals to the Company and its affiliates (the "**Customer**") in accordance with the following scope: (i) categories of data subjects – Customer's employees, customers, contractors and service providers; (ii) categories of Personal Data - name, contact information (including addresses, emails and telephone numbers), IP address, location information, images, video and system, facility, device or equipment usage data; and (iii) special categories of Personal Data – Honeywell does not process any special categories of Personal Data; (together, the "**Customer Personal Data**"). Unless otherwise agreed in separate agreements or the Company Agreement, to the extent the applicable privacy laws recognize the roles of "data controller" and "data processor" as applied to Personal Data then, as between Honeywell and Customer (together, the "**Parties**" and each, a "**Party**"), Customer acts as data controller and Honeywell acts as data processor and shall process Customer Personal Data solely on behalf of and in accordance with Customer's documented instructions, this Agreement, the Company Agreement and/or applicable privacy laws and only to the extent, and for so long as necessary, to provide, protect, improve or develop the Software or Portals and/or related services and perform rights and obligations under this Agreement or the Company Agreement. The performance of this Agreement or the Company Agreement includes the processing of Customer Personal Data in order to improve Honeywell's and its affiliates' solutions and offering related to the services provided under this Agreement or the Company Agreement. For the purposes of clarity, Honeywell will only retain, use and disclose Customer Personal Data as permitted or required under this Agreement, the Company Agreement and applicable privacy laws and Honeywell will not sell any Customer Personal Data to any third party. Both, Honeywell and the Customer, shall comply with their obligations under applicable privacy laws including in their respective roles as data controller and data processor.
Customer authorizes Honeywell to share Customer Personal Data with sub-processors (including affiliates, intermediaries and service providers) located in any jurisdiction in connection with this Agreement or the Company Agreement, provided Honeywell uses legally enforceable transfer mechanisms and contractually requires sub-processors to abide by terms no less restrictive that those in this Agreement or the Company Agreement with regards to processing of Customer Personal Data. Honeywell shall have no liability for any

losses, costs, expenses or liabilities arising from or in connection with processing of Customer Personal Data in compliance with this Agreement or the Company Agreement or otherwise in compliance with Customer's written instructions. Honeywell shall refer all data subject requests to exercise rights under applicable privacy laws to Customer and —to the extent required by applicable privacy laws— shall provide reasonable assistance to enable Customer to comply with such requests, enable data security, respond to complaints or inquiries, and to conduct any privacy impact assessments and prior consultations with supervisory authorities, provided Customer reimburse all reasonably incurred costs. Upon termination of this Agreement or the Company Agreement, Honeywell shall delete or anonymize all Customer Personal Data, except Honeywell may retain Customer Personal Data if required or permitted by applicable law, e.g. for compliance, audit or security purposes, or as requested by mandatory data retention requirements (e.g. for tax or accounting purposes). In case Honeywell processes Customer Personal Data relating to data subjects in the European Economic Area ("**EEA**"), Switzerland or Philippines, both the Customer and Honeywell agree as follows: (I) if Honeywell believes any instruction from Customer will violate applicable privacy laws, or if applicable law requires Honeywell to process Customer Personal Data not in line with Customer's documented instructions, Honeywell shall notify Customer in writing, unless the applicable law prohibits such notification on important grounds of public interest; (II) Honeywell shall upon request make available to Customer the identity of sub-processors and notify any intended addition or replacement and Customer shall have 5 business days to object after receipt of the notification. If Customer objects and the Parties do not resolve within 1 month following notification of the same to Honeywell, Honeywell may terminate this Agreement or the Company Agreement without penalty on written notice; and (III) Honeywell shall ensure its personnel processing Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Customer hereby authorizes Honeywell to transfer Customer Personal Data to locations outside of its country of origin for the performance of this Agreement or the Company Agreement, provided that such transfer shall be affected by legally enforceable mechanisms for transfers of Personal Data as may be stipulated by applicable privacy laws. In particular, the following provisions for data transfers shall apply: (i) in case the Honeywell contracting entity is located within the EEA and will transfer (or otherwise make available) Customer Personal Data to a sub-Processor outside the EEA for the performance of this Agreement or the Company Agreement, the Parties agree as follows: Customer hereby authorize Honeywell to act as its agent for the limited purpose of binding Customer as principal, in the capacity of "data exporter", to a data transfer agreement with a sub-processor comprising the Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries adopted by the European Commission ("**SCC**"). For the avoidance of doubt, the Customer will at all times remain as the data controller and determine the purposes and the essential means of the processing, and the Customer will receive the full benefit as a data exporter from the warranties and undertakings given by any third party acting as the "data importer" under the SCC; and (ii) in case Customer is located within the EEA or Switzerland, the Honeywell contracting entity is not located within the EEA or a country which is subject to an adequacy decision by the European Commission and Honeywell will process Customer Personal Data relating to data subjects in the EEA or Switzerland, the Parties agree as follows: Customer and Honeywell hereby acknowledge and agree that the SCCs (located at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, shall be deemed to have been signed by Customer, in the capacity of "data exporter", and by Honeywell, in the capacity of "data importer" (as those terms are defined in the SCC), and that the SCC are hereby incorporated into this Agreement or the Company Agreement in their entirety as if set out in full as an appendix to this Agreement or the Company Agreement. The Parties acknowledge that the information required to be provided in the appendices to the SCCs is set out in this data privacy section. If there is a conflict between the provisions of this Agreement and the Company and the SCC, the SCC shall prevail. Honeywell will use reasonable technical and organizational measures to protect Customer Personal Data and follow industry-standard security practices. A list of the technical and organizational measures implemented by Honeywell is attached to this Agreement or to the Company Agreement as Appendix 5. Customer is responsible for costs incurred due to unauthorized use or access through Customer's account credentials or systems.

Where the processing of Customer Personal Data is subject to the GDPR, the Parties agree as follows: Honeywell can demonstrate its compliance with its obligations stipulated in the GDPR by provision of suitable evidence, e.g. formal certification such as SOC2 Type 1 and Type 2 (or equivalent). Only in exceptional cases, e.g. when Honeywell is not able to provide such suitable evidence, Customer may audit Honeywell's compliance with such obligations once per year at the applicable facility ("**Audit**") according to

applicable privacy laws. Audits will only be performed following Customer's written request at least 90 days prior to the proposed start date and Customer providing a reasonably detailed audit plan describing the proposed scope, start date and duration. The Parties will work in good faith to agree on a final audit plan. Audits will be conducted during Honeywell's regular business hours, subject to the published policies of the audited facility, and may not unreasonably interfere with business activities. The personnel conducting the Audit on behalf of Customer or any third party auditor mandated by Customer shall enter into an appropriate written confidentiality agreement acceptable to Honeywell prior to conducting the Audit and shall be accompanied by at least one member of Honeywell staff at all times. If the information required for an Audit is not contained in existing reports, Honeywell will make reasonable efforts to provide it to the auditor. To preserve the security of Honeywell organization and customers, Honeywell reserves the right to not share information that could expose or compromise its security, privacy, employment policies or obligations to other customers or third Parties or share confidential information. Records may not be copied or removed from Honeywell facilities. Customer will generate and provide Honeywell with an audit report within 3 months after the Audit. All information obtained or generated in connection with an Audit, including audit reports, shall be kept strictly confidential and may only be used for the purposes of confirming Honeywell's compliance with its obligations stipulated in the GDPR. Customer pays or reimburses Honeywell's reasonable costs for allowing for and contributing to Audits.

Honeywell shall evaluate and respond to any confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized access, disclosure or use of Customer Personal Data due to a breach of Honeywell's obligations under this data privacy section (each a "**Security Incident**"), and will work with Customer and where necessary with outside regulatory and law enforcement authorities to respond to and mitigate the adverse effects of a Security Incident. Where it is determined a Security Incident has occurred, Honeywell shall notify Customer without undue delay and as relevant information becomes available to assist Customer in meeting its potential reporting or notice obligations under applicable law. Customer shall reimburse Honeywell's reasonably incurred costs as a result of providing such information if and to the extent that any such Security Incident does not directly result from Honeywell's breach of its obligations under this Agreement or the Company Agreement and/ or to the extent that any such Security Incident or the circumstances giving rise to them are contributed to or caused by any breach of this Agreement or the Company Agreement by the Customer. Customer shall work with Honeywell in good faith to develop any related public statements or notices resulting from a Security Incident. Provided Honeywell is in material compliance with its obligations regarding Security Incidents, Honeywell's obligations set out herein are Honeywell's sole obligations, and Customer's sole and exclusive remedy, for Security Incidents.

Each Party may process Personal Data in the form of business contact details relating to individuals engaged by the other Party or its affiliates ("**Staff**") for the purposes of performing each Party's obligations under this Agreement or the Company Agreement and managing the business relationship between the Parties, including their business communication. Any processing of such Personal Data by the Parties will be done as data controllers in accordance with the terms of this Agreement, the Company Agreement and applicable privacy laws. Each Party will take appropriate technical and organizational measures to protect such Personal Data against Security Incidents and shall securely delete it once no longer required for the purposes for which it is processed. Each Party shall be responsible for providing necessary information and notifications required by applicable privacy laws to its Staff. Where required under applicable privacy laws, each Party shall inform its own Staff that they may exercise their rights in respect of their Personal Data against the other Party by submitting a written request with proof of identity to that other Party.

Regarding the personal data you directly provide to Honeywell in the context of this Agreement or that provided by your employer (which may include, in general and among others, your name, surname, position in the Company and contact details, such as your email address), Honeywell will process the same as data controller in order to manage and control the contractual relationship with your employer as well as to comply with applicable laws. The processing of such personal data is necessary for such purposes and Honeywell will rely in its legitimate interest in the formalization and execution of the contractual relationship with your employer (after carrying out a balancing test —upon request— and insofar they are not overridden by your rights and interests) and, if applicable, in complying with applicable laws (commercial laws, tax laws, etc.). Your personal data will be retained for the duration of this Agreement and, afterwards, for the period required for the

protection against potential legal and contractual actions and until the expiration of such actions. You may exercise your rights with regards to your personal data, such as your rights of access, rectification, erasure, data portability and restriction of processing to the attention of Honeywell's Data Protection Officer at the following address: HoneywellPrivacy@honeywell.com. You can also address to the competent data protection supervisory authority and claim or query on data protection matters.

6. **Open Source.** Certain components of the Software or Portals may incorporate open source software ("**Open Source**") and to the extent required by the licenses covering Open Source, the terms of such licenses will apply to such Open Source in lieu of this Agreement. To the extent the licenses applicable to Open Source: (i) prohibit any restriction in this Agreement with respect to such Open Source, such restriction will not apply to such Open Source; and (ii) require us to make an offer to provide source code or related information in connection with the Open Source, such offer is hereby made. You acknowledge receipt of notices for Open Source.

7. **Compliance**. You must comply with all laws applicable to your use of the Software and Portals including data privacy or localization, anti-bribery and export control laws (i.e. export to embargoed, prohibited or restricted countries or access by prohibited, denied and designated persons) and your rights to use the Software and Portals is subject to such compliance. For purposes of FARs, DFARs and access by governmental authorities, the Connected Solutions and Input Data are "commercial computer software", "commercial computer software documentation" and "restricted data" provided to you under "Limited Rights" and "Restricted Rights" and only as commercial end items.

8. **Term, Suspension**. This Agreement commences upon the first to occur of when you click agree (or similar term) or download/install/access and continues until termination or expiry of the relevant Company Agreement pursuant to which your access to our products and services is granted. We may terminate this Agreement if you breach it, your use is fraudulent or may subject us to potential liability, we are entitled to terminate or suspend rights under the Company Agreement, your access is not authorized or we suspend or end operation or use of the Portals or Software.

9. **Warranty Disclaimer.** THE SOFTWARE AND PORTALS ARE PROVIDED WITH NO WARRANTIES OR REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE, ON BEHALF OF OURSELVES AND LICENSORS AND SUPPLIERS, EXPRESSLY DISCLAIM ALL SUCH WARRANTIES AND REPRESENTATIONS INCLUDING MERCHANTABILITY AND FITNESS FOR PURPOSE. WE DO NOT WARRANT THAT THE SOFTWARE OR PORTALS WILL OPERATE WITHOUT INTERRUPTION, OR BE ERROR FREE.

10. **Limitation of Liability.** HONEYWELL WILL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS OR REVENUES. HONEYWELL'S CUMULATIVE, AGGREGATE LIABILITY TO YOU WILL NOT EXCEED $100. THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION APPLY TO ALL CLAIMS AND CAUSES OF ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF FORM, WHETHER IN CONTRACT, TORT OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES.

11. **Governing Law and Dispute Resolution.** This Agreement and any disputes arising under or pursuant to it shall be governed by and construed in accordance with the substantive laws of the jurisdictions set out below, without regard, in each case, to conflicts of laws principles, and excluding the United Nations Convention on the International Sale of Goods of 1980 (and any amendments or successors thereto). The applicable jurisdictions are as follows: (i) if the Honeywell contracting entity is formed in the United states, this Agreement shall be governed by and construed in accordance with the substantive laws of the State of New York, and the federal or state courts in New York, New York will have exclusive jurisdiction of any dispute; (ii) if both parties are domiciled in the People's Republic of China (excluding Taiwan), the laws of The People's Republic of China will govern and; any dispute will be subject to binding arbitration in Shanghai under the rules of the China International Economic Trade Arbitration Commission ("CIETAC"), using three arbitrators, one each selected and appointed by the respective parties within 30 days of the arbitration request date and the third selected by the Chairman of CIETAC; and (iii) in all other cases, the laws of England and Wales will govern and disputes will be finally resolved by a panel of three arbitrators in accordance with the Rules for Arbitration of the International Chamber of Commerce, with London, England

as the place of arbitration. The language of all arbitrations under any subsection of this Clause will be English. Judgment upon any award rendered by the arbitrators identified may be entered in any court having jurisdiction. Until the award is entered, either party may apply to the arbitrators for injunctive relief and/or seek from any court having jurisdiction, interim or provisional relief if necessary to protect the rights or property.

12. **Miscellaneous.** This Agreement and the rights granted herein are not assignable or transferrable by you. We may assign or transfer this Agreement or any rights in it with or without notice to you. Unenforceable provisions will be reformed to permit enforceability with maximum effect to the original intent. Waiver of a breach is not waiver of other or later breaches. The parties are independent contractors of the other. If required by our written contract with them, certain of our licensors are third party beneficiaries of this Agreement. The controlling version of this Agreement is this English language version regardless translation. The word “including” is exemplary meaning “including without limitation” or “including, but not limited to.” The words “shall,” “will,” and “must” are obligatory while “may” is permissive, giving a right, but not obligation.