

CONNECTED SOLUTION • GENERAL TERMS AND CONDITIONS

We offer software-, platform- and infrastructure-as-a-service, and related software, hardware and services all designed to connect facilities, devices and equipment and their control systems to analyze, display, process and store data deployed remotely through the cloud and accessible via online portals, mobile apps or interfaces such as https, VPN or API ("**Services**"). These General Terms and Conditions ("**GTCs**") relate to your use of and access to the software-as-a-service portal in respect of the Services (the "**Connected Solution**"). Certain capitalized words and phrases in these GTCs have special meanings that are provided where they first appear or in Section 19.

1. Connected Contracts. The specific Connected Solution for which you purchase Use Rights will be identified in a print or electronic document which may be identified as "proposal", "order" or similar name (the "**Order Terms**"), to which these GTCs are attached. Order Terms should identify each transaction's contracting entities, pricing and related provisions and may reference or link to supplemental terms, agreements or policies, and references to Order Terms includes such documents. Once accepted by us in writing, such Order Terms, together with these GTCs form a single contract (the "**Connected Contract**").

2. Use Rights. Subject to payment of agreed fees and strict compliance with the terms of access and acceptable use, you will be provided with: (a) remote access to the Connected Solution; (b) a personal, revocable, non-exclusive, non-assignable, non-transferable license to: (i) download, install, and use software we provide solely to operate the Connected Solution; and (ii) use Connected Solution documentation as reasonably required in connection with its use (collectively, "**Use Rights**"). Use Rights extend to updates provided as Support. Order Terms may list metrics, including user number, data volume, sensors or other means to measure usage or fees (the "**Usage Metrics**"). Use Rights are subject to Usage Metrics and restrictions in the Connected Contract. If you exceed Usage Metrics, we may suspend access until you pay required fees. Your Users may exercise your Use Rights, provided that, you must bind Users to these GTCs. You are responsible for Users' compliance with, and any breach of the GTCs as well as their acts and omissions. You may only resell Use Rights to third parties or make copies of the Connected Solution (other than for back up purposes) if the terms of these GTCs are imposed on such third parties to which you resell or provide copies, and you will remain responsible for all of their acts and omissions.

3. Accounts. You and Users may be required to download a mobile app, or visit an internet portal or site, through which you will access the Connected Solution and set up accounts including our issuance or your creation of authentication credentials. In operating your account you and Users must: (i) maintain strict confidentiality of user names, passwords or other credentials; (ii) not allow others to use your credentials or access your account; (iii) immediately notify us of any unauthorized use or breach of security related to your account; (iv) submit only complete and accurate information; and (v) maintain and promptly update information if it changes. We have no responsibility with respect to any actions or inactions of your Users, and you will be responsible for access by any party you authorize. We may use rights management features (e.g. logout) to prevent unauthorized use.

4. Acceptable Use. The Use Rights are the only acceptable use of the Connected Solution. You shall not use the Connected Solution for purposes of, or in connection with: (a) reverse engineering, making machine code human readable or creating derivative works or improvements; (b) interfering with its security or operation (including probing, scanning or testing the vulnerability of any security measures or misrepresenting transmission sources); (c) creating, benchmarking or gathering intelligence for a competitive offering; (d); infringing another's IPR; (e) employing it in hazardous environments requiring fail-safe performance where failure could lead directly or indirectly to personal injury or death or property or environmental damage; or (f) any use that would reasonably be expected to cause liability or harm to us or our customers.

5. Set Up, Support. Initial set up and configuration are provided if stated in the Order Terms. We will manage, maintain and support the Connected Solution ("**Support**") in accordance with the policies specified in the Order Terms or, if none are specified we will use commercially reasonable efforts to maintain the Connected Solution, repair reproducible defects and make available as a whole 99% of the time 24x7x365 subject to scheduled downtime, routine and emergency maintenance and force majeure. Support excludes device or third party application set up unless stated in the Order Terms. 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.

6. Fees, Tax. Fees are invoiced in advance on the first business day of each subscription period or as otherwise set out in the CSA with invoices payable within 30 days of invoice date. We reserve the right to charge additional fees for new or improved features or functions. Payments are in GBP (unless agreed otherwise by us in writing) and must be made in accordance with the "Remit To" field on each invoice. Disputes as to invoices must be accompanied by detailed supporting information and if not raised within 15 days of invoice receipt are deemed waived. We reserve the right to correct any inaccurate invoices which must be paid by the original invoice payment due date or the issuance date of the corrected invoice, whichever is later. Your obligation to pay is not contingent on our performance under different agreements or your receipt of payment from other parties and you may not set

off any invoiced amounts against any amount due from us. Fees do not include applicable taxes all of which are your responsibility and payable by you (excluding taxes on our income). We may invoice sales and related taxes (e.g. VAT) unless you provide a valid exemption certificate in advance. For material breach or if you are delinquent in payment to us we may, without prejudice to any other legal or equitable remedies, suspend performance and late fees up to 1.5% and collection costs including reasonable attorneys' fees. We may take remedial action or impose additional credit obligations if there is an adverse change in your creditworthiness. We are not liable for increased costs caused by you or your service providers and may reasonably adjust fees to reflect any such costs.

7. Term, Termination. Your Use Rights commence on the effective date of, and continues for the duration specified in, the Order Terms unless terminated earlier (the "**Term**"). We may terminate your Use Rights if you commit a material breach of a Connected Contract and fail to cure within 30 days of written notice. We may also terminate your Use Rights upon written notice if: (i) you are insolvent, attempt to obtain protection from creditors or wind down operations; (ii) Use Rights were granted at no charge, use is fraudulent or if continued use would subject us to third party liability; or (iii) if we cease making the Connected Solution available to third parties. We may suspend Use Rights if we determine that you or Users are or may violate the Connected Contract. During suspension, you and Users will not have access to all or part of the Connected Solution and may be unable to access Input Data. Upon termination or expiry: (a) you must pay amounts due and delete all copies of Connected Solution and credentials; and (b) if requested by disclosing party, receiving party must return or destroy all Confidential Information and certify the same in writing; except for automatically generated backup copies, anonymized Input Data or if maintained for legal purposes. Sections 4 and 7 to 16 and those portions of these GTCs that by their nature should survive, survive termination or expiration.

8. IP & Data. You agree that **Honeywell** and its licensors have rights, title and interest, including all intellectual property rights (including copyrights, trademarks and patents), proprietary rights (including trade secrets and know-how), and moral rights (including rights of authorship and modification) throughout the world ("**IPR**") in and to the Connected Solution and all of their derivative works and improvements. 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 Connected Solution ("**Input Data**"). You agree that parties identified in the Order Terms, Channel Dealers, Honeywell and its Affiliates ("**Data Rights Parties**") have the right to retain, transfer, disclose, duplicate, analyze, modify and otherwise use Input Data to provide, protect, improve or develop their products or services. Data Rights Parties may also use Input Data for any other purpose provided it is in an anonymized form. Personal Data within Input Data shall only be used in accordance with the privacy terms below. All information, analysis, inventions and algorithms derived from Input Data by Honeywell or its Affiliates (but excluding the Input Data itself) and any IPR obtained related thereto, are owned exclusively and solely by Honeywell or its Affiliates and are Honeywell or its Affiliates' confidential information. 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 Data Rights Parties' use of Input Data. You waive any IPR in suggestions or feedback you or any User provides regarding the Connected Solution. You and Users shall not remove, modify or obscure any proprietary rights notices on the Connected Solution.

9. Confidentiality. All information one party receives from the other in its performance of a Connected Contract that is generally not known ("**Confidential Information**") shall be held in strictest confidence and shall not, without the written consent of the disclosing party, be used or disclosed except to the receiving party's Affiliates, employees, Channel Dealers and service providers who are bound to substantially similar obligations of confidentiality and have a need to know. Each party will be responsible for any breaches of the confidentiality obligations by its Affiliates, employees Channel Dealers or service providers or Users. Receiving party will keep all Confidential Information confidential for 10 years from disclosure. Except as agreed in writing, information will not be Confidential Information unless (a) marked "CONFIDENTIAL" or "PROPRIETARY" or similar marking at the time of disclosure; or (b) disclosed orally or visually but identified as confidential at the time of disclosure and designated as confidential in writing within 30 days of disclosure summarizing the Confidential Information sufficiently for identification; or (c) it should reasonably be understood to be confidential given the nature of the information as sensitive and non-public information. Confidential Information excludes information that: (a) was already known to recipient without restriction; (b) is publicly available through no fault of recipient; (c) is rightfully received by recipient from a third party without a duty of confidentiality; or (d) is independently developed. A party may disclose Confidential Information when compelled to do so by law if it provides prior notice to the other party and reasonable opportunity to contest or limit disclosure, unless a court orders that the other party not be given notice. You acknowledge and agree that the Connected Contract contents and the internal operation, workings and processes and performance of the Connected Solution (including results of any evaluation or trial) are Honeywell's Confidential Information. Input Data is your Confidential Information except if in an anonymized form that does not identify you or any individual.

10. 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 than 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.

11. Security. (i) We will use commercially reasonable administrative, physical and technical safeguards to protect Personal Data and Input Data and follow industry-standard security practices; and (ii) following a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized access, disclosure or use of your Personal Data or Input Data we will notify you without undue delay and as relevant information becomes available to assist you in meeting your potential reporting or notice obligations under applicable law and you will work with us in good faith to develop any related public statements or required notices. You will implement commercially reasonable administrative, physical and technical safeguards to protect Connected Solution and follow industry-standard security practices. You are solely responsible for costs and liability incurred due to unauthorized use or access through your or Users account credentials or systems.

12. Open Source. We may use open source software (“OSS”) and to the extent required by the licenses covering OSS, the terms of such licenses will apply to such OSS in lieu of this Agreement. To the extent the licenses applicable to OSS: (i) prohibit any restriction with respect to such OSS, such restriction will not apply to such OSS; and (ii) require us to make an offer to provide source code or related information in connection with the OSS, such offer is hereby made. You must comply with all laws applicable to use of Connected Solution and Use Rights are subject to such compliance.

13. Warranty, Disclaimer. WITHOUT LIMITING OUR OBLIGATIONS UNDER ANY SPECIFIED SUPPORT OR SECURITY POLICY THE CONNECTED SOLUTION AND SUPPORT 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 WARRANTIES AND REPRESENTATIONS INCLUDING MERCHANTABILITY AND FITNESS FOR PURPOSE. WE DO NOT WARRANT THAT THE CONNECTED SOLUTION WILL MEET YOUR REQUIREMENTS, OR THAT THEY OR THE SUPPORT WILL OPERATE WITHOUT INTERRUPTION, OR BE ERROR FREE.

14. Limitation of Liability. EXCEPT FOR UNCAPPED EVENTS AND AS EXPRESSLY SET OUT IN THE CONNECTED CONTRACT, NEITHER PARTY WILL BE LIABLE FOR INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS AND REVENUES AND EACH PARTY’S CUMULATIVE, AGGREGATE LIABILITY TO THE OTHER, WILL, OTHER THAN FOR FEES PAYABLE, BE LIMITED TO DIRECT DAMAGES IN AN AMOUNT EQUAL TO THE GREATER OF: (a) TOTAL AMOUNTS PAID OR PAYABLE UNDER THE CONNECTED CONTRACT DURING THE SIX MONTHS IMMEDIATELY PRECEDING THE ASSERTION OF ANY CLAIM; AND (b) £5,000. OUR LIABILITY UNDER EVALUATION OR TRIAL RIGHTS IS LIMITED TO £1,000. The following “**Uncapped Events**” are not subject to the cap or exclusions: (i) claims for injury or death resulting from negligence; (ii) claims resulting from either party’s gross negligence, fraudulent or willful misconduct; (iii) breach of confidentiality obligations (except in relation to Input Data and Personal Data for which the cap and exclusions apply); (v) a party’s indemnity obligations; and (vi) infringement, misappropriation or violation by a party, its Affiliates or Users, of the other party’s or its Affiliates IPR. All claims and causes of action must be brought within the earlier of six months of being discovered or one year after end of the Connected Contract. Nothing precludes a party from seeking declaratory, injunctive or other equitable relief from a court of competent jurisdiction. THE LIMITATIONS AND EXCLUSIONS APPLY TO ALL CLAIMS AND CAUSES OF ACTION ARISING OUT OF OR IN RELATION TO THE CONNECTED CONTRACT REGARDLESS OF FORM.

15. Indemnification. We will, at our cost and expense, defend your [Indemnitees](#) from all [Covered Proceedings](#), and hold them harmless from and pay or reimburse all [Covered Liabilities](#) arising out of claims by third parties that your use of the Connected Solution under the Use Rights infringed or misappropriated their IPR; provided that, with respect to patents, our obligation is limited to U.S. patents issued before the Connected Contract becomes effective. We have no indemnification obligations to the extent a claim arises from: (a) Input Data; (b) your use of the outputs of the Connected Solution; (c) use other than under Use Rights; (d) combining Connected Solution with goods or technology or services not supplied by us; (e) modifications by anyone other than us; or (f) compromise or settlement made by you without our written consent. If the Connected Solution is held, or we believe it may be, infringing, we will undertake at least one of the following with respect to the allegedly infringing materials: (i) procure a license to allow your use; (ii) modify them to make them non-infringing; or (iii) procure a license to a reasonable substitute product. If we cannot do one these after a reasonable period, we may terminate the Connected Contract by notice and refund a pro-rata portion of pre-paid fees received during the applicable period. The foregoing are our only liabilities and your Indemnitees’ only remedies for claims Connected Solution infringe, misappropriate or violate IPR. You will, at your cost and expense, defend our Indemnitees against all Covered Proceedings, and hold them harmless from and pay or reimburse all Covered Liabilities, arising out of out of claims by third parties related to: (a) possession, processing or use of Input Data or Personal Data in relation to the Connected Contract; or (b) you or Users’ infringement, misappropriation or violation of our or a third party’s IPR (except if caused by your authorized use of the Connected Solution). The Indemnitees shall notify the indemnifying party in writing of a claim or other event requiring defense or indemnification promptly upon becoming aware thereof. The indemnifying party shall have the reasonable right to control the defense and/or settlement of each claim and the Indemnitees shall provide reasonable assistance.

16. Compliance: You must comply with all laws and regulations applicable to your use of Connected Solution 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 or designated persons) and your rights to use the Connected Solution is subject to such compliance. For purposes of FARs, DFARs and access by governmental authorities, the Connected Solution 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.

17. Channel Dealers. We may appoint parties to resell or support Connected Solutions, and/or distribute, integrate or bundle them with devices, systems or equipment (“**Channel Dealers**”). Channel Dealers are independent entities who unilaterally set pricing and related terms which may include “first line” support and we are

not responsible for their acts, omissions, statements or warranties. Channel Dealers access a Connected Solution on your behalf and are your Users. You may remove any Channel Dealers from accessing as your User either through the Connected Solution or by contacting us. We are not responsible for acts or omissions of third parties you retain. If we end our contractual relationship with a Channel Dealers through whom you purchased or operate the Connected Solution, you may designate a successor by provision of written notice to us within 10 business days of becoming aware they are no longer our Channel Dealers. If we do not receive such notice from you, we may: (a) terminate your Use Rights; or (b) transfer you to a party we select. If the predecessor had been paying fees on your behalf and fails to pay us, you are responsible for payment until transition to the successor is complete.

18. Law, Dispute. These GTCs and any disputes arising under or pursuant to them 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 We, the contracting entity are 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. Such award will be payable in the currency of the Connected Contract. 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.

19. Miscellaneous. Any descriptions of future product direction or intended updates (including new or improved features or functions) other than the features and functions deployed as of date of this Agreement are intended for information purposes only and are not binding commitments on us to deliver any material, code or functionality. The development, release and timing of any such updates is at our sole discretion unless agreed otherwise in writing. We may assign or transfer a Connected Contract or any rights in it on 10 business days written notice. During the Term and 24 months after, we or our designee can, during normal business hours upon reasonable notice, access, inspect and audit, your compliance with the Connected Contract and you will furnish such information and access to personnel as we may reasonably request. We have the right to monitor usage. You may not assign or transfer a Connected Contract without our prior written consent. Notices must be sent by reputable overnight courier to a party's address specified in the Order Terms and deemed given three business days after sending. Failures in performance beyond a party's reasonable control are excused (except failure to pay). 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 and waivers must be in writing. 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 the Connected Contract. The controlling version of these GTCs is this English language version regardless translation. Each Connected Contract is the entire agreement between us with respect to the Connected Solution identified, superseding all prior or contemporaneous written and verbal agreements or proposals and cannot be modified except by written agreement. If you use a Connected Solution with equipment separately purchased from us or a third party, these GTCs, followed by the Order Terms takes precedence for all matters involving the Connected Solution and over any terms contained in the documentation or terms of sale for such equipment. Conflicts among the Connected Contract will be resolved by giving precedence as follows: (a) GTCs; (b) Order Terms; and (c) other supplemental terms, agreements or policies referenced in the Order Terms. Customer purchase orders are identified only to authorize payment and are not a part of the Connected Contract. The following definitions apply:

"Affiliate" means any entity that controls, is controlled by, or is under common control with, another entity. An entity "controls" another if it owns directly or indirectly a sufficient voting interest to elect a majority of the directors or managing authority or otherwise direct the affairs or management of the entity.

"Covered Proceedings" means demands, suits, claims, actions, proceedings or investigations that result in, or occur because of indemnified claims.

"Honeywell" means Honeywell Inc. and Affiliates.

"User" means you, your employees or service providers or any third party/person accessing the Connected Solution

under your Use Rights or on your behalf including any Channel Dealers and any party to which you on-sell such Use Rights as permitted in the Order Terms. **"We"**, **"us"** and **"our"** means the other party who executes or otherwise assents to the Order Terms.

"You", **"your"** and their variants mean collectively, the contracting entity executing or otherwise assenting to the Order Terms as well as any individual who acting on behalf of such entity has administrator or similar rights to the Connected Solution. References to "you" and "your" in the context of Use Rights restrictions, conditions and related obligations include Users.