HONEYWELL TECHNOLOGIES END USER LICENSE AGREEMENT FOR SAAS

November 1, 2026

IMPORTANT NOTICE, PLEASE READ CAREFULLY.

This End User License Agreement ("**EULA**") is a legal agreement that sets forth the rights and obligations governing use of this software-as-a-service, hosted platform, or online or cloud-based service or feature made available by Honeywell, including any updates thereto (collectively, the "**SaaS**") and related documentation ("**Documentation**") by and between the business entity using the SaaS ("**User**") and Honeywell International Inc. or its local affiliate(s) specified in the print or electronic document identified as "proposal", "order", "agreement" or similar name ("**Order**") related to the SaaS ("**Honeywell**") (collectively, the "**Parties**" and each a "**Party**")**.** Unless otherwise mutually agreed upon by the Parties, this EULA takes precedence over any other terms and conditions, documents or agreements between the Parties governing the use of the SaaS.

BY CLICKING "ACCEPT" AND/OR USING THE SAAS AND DOCUMENTATION, YOU, AS THE PERSON ACCESSING THIS SAAS ON BEHALF OF USER, REPRESENT: (1) THAT YOU HAVE READ AND AGREE TO THE TERMS OF THIS EULA; (2) YOU ARE ENTERING INTO THIS EULA ON BEHALF OF USER; AND (3) YOU AGREE THAT YOU HAVE THE AUTHORITY TO BIND USER TO THE TERMS OF THIS EULA. IF YOU DO NOT HAVE AUTHORITY TO ENTER INTO THIS EULA ON BEHALF OF USER AND BIND USER TO THE TERMS OF THIS EULA OR DO NOT AGREE TO ITS TERMS, DO NOT CLICK "ACCEPT" OR USE THE SAAS OR DOCUMENTATION.

1. **License Rights**. Subject to User's compliance with the terms and conditions of this EULA and payment of applicable fees, Honeywell: (a) will provide User access to the SaaS via means authorized and provided by Honeywell (which may include an online portal or interface such as https, VPN or API); and (b) hereby grants to User a limited, non-transferable, non-exclusive, revocable, non-sublicensable right and license to (i) access and use the SaaS through such means; (ii) download, install, update and allow Honeywell to update (when applicable), and use any software Honeywell provides solely in support of User's usage of the SaaS; (iii) use Documentation for the SaaS as reasonably required in connection with the SaaS; and (iv) use any output of the SaaS, in each case solely for User's internal business purposes including, for example, use by User's authorized employees, contractors, or representatives who have been informed of and agree to comply with the terms of this EULA ("**Authorized End Users**") (collectively, "**SaaS Use Rights**"). SaaS Use Rights continue for the period stated in the applicable Order, or if no duration is stated, for 12 months from the effective date of the Order. An Order may list metrics, including user number, data volume, sensors or other means to measure usage or fees ("**SaaS Usage Metrics**"). SaaS Use Rights are subject to SaaS Usage Metrics and any other restrictions in this EULA. If User exceeds SaaS Usage Metrics, Honeywell may suspend User's access until User pays all required fees to Honeywell. Authorized End Users may exercise SaaS Use Rights only if User binds them to the terms of this EULA. User is responsible, and Honeywell has no liability, for Authorized End Users' compliance with this EULA and for any breach, act or omission by them. User may not resell SaaS Use Rights and may not make copies of the SaaS, in each case except as agreed by Honeywell in writing.

2. **Acceptable Use.** User will not (and will not authorize, encourage or cooperate with any third party to): (a) reverse engineer, modify, adapt, make machine code human readable or create derivative works or improvements of the SaaS; (b) circumvent or interfere with the technical protections, security or operation (including disrupting, interacting in an unauthorized manner, probing, scanning or testing the vulnerability of security measures or misrepresenting transmission sources) of the SaaS; (c) perform competitive analysis (including benchmark testing) or create, train or improve a substantially similar product or service to the SaaS; (d) access or use the SaaS in a manner that infringes another's intellectual property rights; (e) employ the SaaS in hazardous environments or inherently dangerous applications, including any product, part, service or other application that could result in death or personal injury, or requiring fail-safe performance where failure could lead directly or indirectly to personal injury or death or property or environmental damage; (f) employ the SaaS as (or as a substitute for) a third-party monitored emergency notification system; (g) access or use the SaaS in a manner that would reasonably be expected to cause liability or harm to Honeywell or Honeywell's customers or breach this EULA; (h) employ the SaaS for critical control of environments,

emergency situations, life safety or critical purposes; (i) upload to or use the SaaS to store or transmit infringing, obscene, threatening, libelous or otherwise unlawful or tortious material, including material that is harmful to children or that violates third-party rights, or use the SaaS for or in connection with any unlawful, harmful or fraudulent use or activities; (j) upload to or use with the SaaS any technical data or software controlled under the International Traffic in Arms Regulations (ITAR) or other Sanctions Laws (as defined in the Compliance Section below); (k) train any machine learning or artificial intelligence algorithm, software or system using the SaaS; or (l) sublicense, distribute or otherwise make available any portion of the SaaS (including any functionality of the SaaS) to a third party. Any violation of the restrictions in this Section will constitute a material breach of this EULA.

3. AI Use Restrictions.

a. "**Honeywell AI**" means a machine-based system designed to operate with varying levels of autonomy (including solving problems and performing tasks), that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the Input Data it receives, how to generate Outputs (defined below) such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. This includes features which incorporate artificial intelligence models or tools made available by Honeywell to User. "AI System" has the meaning given to that term in the EU AI Act. "**High Risk Use**" means any uses of Honeywell AI that could or does: (i) significantly and negatively impact Honeywell's operations or reputation; (ii) significantly and negatively impact intellectual property protections or data security or privacy; (iii) impact the work and lives of User's employees, users, partners, clients, and members of the public; or (iv) present novel or significant legal, compliance, or enterprise risks. This would include high risk AI Systems, which pose significant risk of harm to people's health, safety, or fundamental rights as defined under the EU AI Act. "**Unacceptable Risk Use**" or "**Prohibited Use**" means any use of Honeywell AI that: (i) could have or actually has an effect on the access of an individual to employment or in a manner that could affect an individual's rights under Applicable AI Laws; (ii) could lead to or cause bias or discrimination; or (iii) could lead to errors, omissions or other risks that have the potential to impact safety, fundamental rights of natural persons or affect the safety of tangible or physical property. This includes prohibited uses as defined under the EU AI Act.

b. Without Honeywell's prior written consent, User will not (and will not authorize, encourage or cooperate with any third party to): (i) use any Honeywell AI or Outputs for a High Risk Use or Unacceptable Risk Use; (ii) use Honeywell AI to make automated decisions that may have a detrimental impact on individual rights without appropriate human supervision; (iii) distribute or use the Honeywell AI in any manner except as provided under this EULA; (iv) make modifications to or otherwise create derivative works of or improvements to the Honeywell AI; notwithstanding the foregoing, any such unauthorized works and any intellectual property rights therein, will be deemed to be the sole and exclusive property of Honeywell; (v) circumvent or interfere with the technical protections, security or operation of the Honeywell AI; (vi) assert, or authorize, assist, or encourage any third party to assert, against Honeywell or any Honeywell affiliates, customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding the Honeywell AI; (vii) copy, create, offer, train, or sell any competing AI System, product, service or offering with the same or similar functionality during the term of this EULA; (viii) access or use the Honeywell AI in a manner that infringes another's intellectual property rights; (ix) engage in any conduct that may be detrimental to the Honeywell AI or marketability thereof; (x) use Honeywell AI or Outputs to generate content that violates or promotes violence, hate speech, or harassment, or insults or demeans a person; (xi) generate sexually explicit content or contravene any regulatory safety policies;
(xii) mislead any person into believing that Honeywell AI or Outputs are solely human-generated; (xiii) enter into any agreement which requires User to take any actions that are in conflict with the terms of this EULA; (xiv) sublicense, distribute or otherwise make available any portion of the Honeywell AI (including any functionality of the Honeywell AI) to any third party; or (xv) use or make any Output available to third parties without disclosing that the Output was generated using an AI System.

4. Account Security. User may be required to visit a website through which User accesses the SaaS and sets up accounts including issuance of authentication credentials. In operating User's account, User and Authorized End Users must: (i) maintain strict confidentiality of user names, passwords, or other credentials; (ii) assign accounts to unique individuals and not allow others to use User's credentials or access User's account, including sharing among multiple Authorized End Users; (iii) immediately notify Honeywell of any unauthorized use or breach of security or security incident related to User's account; (iv) submit only complete and accurate information; (v) maintain and promptly update information if it changes; (vi) manage Authorized End Users' access; and (vii) implement Multifactor Authentication (MFA) for

all User accounts that access the SaaS, including those authenticated through federated identity providers or single sign-on. Honeywell may use rights management features (e.g. lockout) to prevent unauthorized use and enforce MFA.

5. **Evaluation Licenses.** Access to the SaaS may be provided to User for beta, demonstration, test, or evaluation purposes (collectively, "**Evaluation Licenses**"). For any Evaluation Licenses, the term shall be limited to ninety (90) days (the "**Evaluation Period**"), unless otherwise agreed to by Honeywell in writing. Evaluation Licenses are limited specifically to use for evaluation or demonstration purposes only, and User agrees not to use such SaaS in a production or non-test environment. User's use of the SaaS under an Evaluation License is provided as-is, without any representations or warranties of any kind, and is at User's sole risk. Honeywell has no obligation to support, maintain, or provide any assistance regarding any Evaluation Licenses. IN NO EVENT WILL HONEYWELL BE LIABLE FOR ANY DAMAGES OF ANY KIND IN RELATION TO ANY EVALUATION LICENSE OR EVALUATION OF THE SAAS BY USER, INCLUDING, WITHOUT LIMITATION, ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, STATUTORY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST DATA, DAMAGE TO SYSTEMS OR EQUIPMENT, OR BUSINESS INTERRUPTION). USER IS NOT ENTITLED TO ANY DEFENSE OR INDEMNIFICATION FOR EVALUATION LICENSES GRANTED PURSUANT TO THIS SECTION.

6. **Audit.** User will maintain complete, current and accurate records documenting the location, access and use of the SaaS or other offerings. During the term of this EULA and for 1 year thereafter (the "**Audit Period**"), Honeywell may: (a) require User to send written certification of compliance with the terms and conditions of this EULA within thirty (30) days; and (b) upon reasonable notice, initiate an audit of User's records and electronic logs to verify User's access to and use of any SaaS or other offerings and User's compliance with the terms and conditions of this EULA, it being understood that any failure to deliver a certificate of compliance on a timely basis will extend the Audit Period and that any audit initiated within the Audit Period may permissibly be completed after the end of the Audit Period. User may not take any steps to avoid or defeat the purpose of any such verification measures and will cooperate with Honeywell to facilitate Honeywell's audit. If any audit reveals any underpayment, if User is purchasing the SaaS or other offerings directly from Honeywell, (i) User will promptly pay Honeywell the underpaid fees and related maintenance and support fees and (ii) if the underpayment is five percent (5%) or more of the fees paid for the SaaS or other offering in any three (3) month period, User will reimburse Honeywell for its audit costs and audit-related expenses.

7. **Updates and Support**. Initial set up and configuration are only provided if stated in User's Order. Honeywell will manage, maintain and support the SaaS ("**SaaS Support**") in accordance with the policies specified in the Order, or if none specified, Honeywell will use commercially reasonable efforts to maintain the SaaS and repair reproducible defects and make the SaaS available subject to scheduled downtime and routine and emergency maintenance. Except as otherwise agreed in writing, User is responsible for the connectivity required to use the SaaS and for maintaining the equipment and infrastructure that connects to the SaaS. Set up and SaaS Support excludes device set up unless stated in the Order. Honeywell reserves the right to modify the SaaS if such modification does not materially diminish the functionality of the SaaS. Honeywell may monitor User's usage of the SaaS. Honeywell may make available to User updates or upgrades to the SaaS in its sole discretion but has no obligation under this EULA to do so, except for security updates that applicable law requires Honeywell to provide, and reserves the right to charge additional fees for new or improved features or functionality or, subject to applicable law, discontinue any SaaS. Honeywell reserves the right to make changes in the SaaS design without obligation to make equivalent changes to any SaaS previously supplied to User.

8. **Security.** Security is governed by policies in the Order or if none are specified Honeywell will use commercially reasonable administrative, physical and technical safeguards designed to protect Personal Data and Input Data (including AI Input Data) and follow industry-standard security practices, as set out in the Security Practices at https://www.honeywell.com/us/en/legal/product-security. User is solely responsible for costs or liability incurred due to unauthorized use or access through User's or Authorized End User's account credentials or systems and for security of on-premises software and hardware.

9. **Intellectual Property Rights.** Except for those rights expressly granted in this EULA, Honeywell and its affiliates and licensors own and reserve all intellectual property rights in and to the SaaS, the Documentation and all of their derivative works, modifications and improvements. The Documentation, SaaS and operation and performance of the SaaS constitute Honeywell's confidential information.

10. **Data Rights.** User retains all ownership and other rights to data and other information that User or persons acting on User's behalf upload, transfer or make available in relation to, or which is collected from User's systems, devices or equipment by, the SaaS ("**Input Data**"). User grants to Honeywell and its affiliates a non-exclusive, transferable, worldwide, perpetual, irrevocable, sublicensable (through multiple tiers), royalty-free and fully paid-up right and license to collect and use the Input Data. Honeywell has the right to retain, transfer, disclose, duplicate, analyze, modify and otherwise use the Input Data to maintain, protect, develop, operate, improve and support Honeywell's products, services or offerings. Honeywell may use Input Data for any other purpose provided it is in an anonymized form that does not identify User or any data subjects. Input Data is User's confidential information. All know-how and information developed by Honeywell and/or its affiliates by processing or analyzing Input Data (but excluding Input Data itself) as well as all results of the Honeywell AI, including software, models, designs, drawings, documents, inventions, and know-how, conceived or developed in connection with the EULA and any intellectual property rights related thereto, are owned exclusively and solely by Honeywell and are Honeywell's confidential information. User has no right or license to intellectual property or inventions provided by Honeywell, except as granted in this EULA. The rights granted to Honeywell with respect to Input Data shall survive termination of this EULA. User has sole responsibility for obtaining all consents and permissions (including providing notices to Authorized End Users or third parties) and satisfying all requirements necessary to permit Honeywell's use of Input Data. Unless agreed in writing, Honeywell does not archive Input Data for User's future use. User consents to any transfer of User's Input Data outside of its country of origin, except that Personal Data is subject to the DPA (as defined in the Data Privacy Section). To the extent User has a right to access Input Data under Regulation (EU) 2023/2854 (the "**Data Act**"), the scope of such data and the technical means for exercising such rights are set forth in applicable documentation. User confirms that it has reviewed and accepts the applicable documentation and waives any right to receive data or metadata not expressly listed therein. User is not entitled to request access to Input Data to which it has direct access through alternative means. Honeywell makes no warranty, express or implied, regarding the accuracy, reliability, compatibility, usability or fitness of any Input Data supplied to User.

11. **Know-how, Feedback.** Honeywell and its affiliates and licensors own and retain all right, title and interest, including all intellectual property rights, in and to: (i) the SaaS and all derivative works, modifications and improvements of the SaaS (including the results of the Honeywell AI); and (ii) know-how and information (excluding AI Input Data and Input Data) that is developed by Honeywell or its affiliates by analyzing Input Data (including AI Input Data) or generated via, or derived from, providing or supporting the SaaS ("**Know-how**"). Subject to User's compliance with the terms and conditions of this EULA (including acceptable use), Honeywell hereby grants to User a limited, non-transferable, non-exclusive, revocable, non-sublicensable right and license to use Know-how solely for its internal business purposes in connection with exercise of SaaS Use Rights. User and Authorized End Users will not remove, modify or obscure any intellectual property-right notices on the SaaS.

    User may voluntarily provide comments, suggestions, enhancement or modification requests, recommendations, proposals, ideas, and other feedback relating to the SaaS or otherwise (collectively, "**Feedback**"). User hereby assigns to Honeywell (and shall cause its employees, contractors, and agents to assign to Honeywell) all right, title, and interest in, and Honeywell is free to use, without any attribution or compensation to any party, any Feedback and intellectual property rights contained in the Feedback, for any purpose whatsoever, whether or not the Feedback was provided at Honeywell's request. Honeywell is not required to hold any Feedback in confidence, pay compensation for any Feedback, implement or use any Feedback, or respond to any Feedback.

12. **AI Input Data and Outputs.**

a. To the extent required by any applicable laws or regulations regarding the use of AI Systems, including but not limited to the European Union Artificial Intelligence Regulation, Regulation (EU) 2024/1689 **("EU AI Act**") ("**Applicable AI Laws**"), and upon User's reasonable request, Honeywell will provide summaries of the data used to train the Honeywell AI.

b. User retains all rights to AI Input Data and though User has a right to use Outputs generated by the Honeywell AI, the

Outputs are owned by Honeywell. User is solely responsible to ensure that all Outputs are checked and validated, that they are fit for User's purpose and that they are in compliance with Applicable AI Laws prior to their use. To the extent any Applicable AI Laws require certain disclaimers or disclosures, User agrees to comply with any such requirement in accordance with User's use of Honeywell AI. Further, due to the nature of an AI System, the Output may not be unique across users and the Honeywell AI may generate or return the same or similar Output to other customers, Honeywell or a third party. If User provides Honeywell with written notice or otherwise decides that User no longer desires to use Honeywell AI, Honeywell is not required to retain the AI Input Data or Outputs used or otherwise processed in connection with the Honeywell AI. "**AI Input Data**" refers to any Input Data applicable to the Honeywell AI, and it also includes a query, prompt, request or other information, content or material submitted to the Honeywell AI for the purpose of generating an Output. **"Output"** means any data, text, content, sound, videos, software code, image, material, information, communication, and other outcome, action or result generated from use of the Honeywell AI.

13. **Data Privacy.**

a. "**Applicable Data Privacy Laws**" means applicable data protection, privacy, breach notification, or data security laws or regulations. "**Data Controller**" means a Party that alone or jointly with others, determines the purposes and means of the processing of Personal Data (as that term or similar variants may otherwise be defined in Applicable Data Privacy Laws). "**Personal Data**" means any information relating to an identified or identifiable natural person or as that term or similar variants may otherwise be defined in Applicable Data Privacy Laws. Personal Data includes (i) relationship data about individuals provided by one Party to the other to manage the relationship between the Parties, and (ii) personally identifiable usage data made available by User to Honeywell in relation to the use of the SaaS for the purposes of providing, improving, or developing Honeywell products and services.

b. Each Party will process the Personal Data of the other as an independent Data Controller in accordance with Applicable Data Privacy Laws. Each Party represents that it has all rights and authorizations to transfer the Personal Data to the other Party (including providing notice). To the extent required by Applicable Data Privacy Laws, each Party agrees to be bound by the terms of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (including the provisions in Module 1) and the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses made under s119A(i) of the UK's Data Protection Act 2018 ("**Controller SCCs**") in its capacity as "data exporter" or "data importer", as applicable, and as those terms are defined therein. The Controller SCCs will be deemed to have been signed by each Party and are hereby incorporated by reference into this EULA in their entirety as if set out in full as an annex to this EULA. The Parties acknowledge that the information required to be provided in the appendices to the Controller SCCs is set out at https://www.honeywell.com/us/en/company/trust. Each Party will implement appropriate technical and organizational measures to protect Personal Data against any security breaches. If there is a conflict between this EULA and the Controller SCCs, the Controller SCCs will prevail. Where applicable law requires changes to the Controller SCCs, those changes will be deemed to have been made without further action from the parties.

c. If Honeywell processes Personal Data on User's behalf, Honeywell's Data Processing Agreement ("**DPA**") at https://www.honeywell.com/us/en/company/trust applies.

14. **Disaster Recovery, Back up.** Honeywell maintains disaster recovery and business continuity plans to manage material loss or failure in the facilities, equipment or technologies used to provide the SaaS ("**Disaster Failure**"). Unless agreed otherwise in writing, Honeywell does not offer account recovery of data separately from that of any other customer and Honeywell is not responsible if backups fail, are incomplete, or could not be performed or Input Data (including AI Input Data) is lost or damaged. In the event of Disaster Failure Honeywell will use commercially reasonable efforts to restore to the most recently available backup. Honeywell's obligations set out in this section are Honeywell's sole obligations, and User's sole and exclusive remedy, for Disaster Failure.

15. **Indemnification.** User will, at User's expense and at Honeywell's option, defend and indemnify Honeywell and its licensors and service providers from and against any third-party claim, suit or proceeding, and pay any final judgments awarded by a court of competent jurisdiction, or reasonable settlement amounts approved in writing by Honeywell, arising out of any claim brought against Honeywell by a third party: (a) alleging that User, its affiliates, or any of its or their employees, agents or subcontractors, infringes such third party's copyright, patent, trademark or trade secret rights including in providing any Input Data (including AI Input Data); (b) arising out of or relating to access or use of, or

inability to access or use, the SaaS by User or its affiliates or any of its or their respective employees, agents and subcontractors; (c) relating to User's use of the Honeywell AI for any High Risk Use or Unacceptable Risk Use; (d) relating to User's failure to comply with this EULA; or (e) related to Honeywell's possession, processing or use of Input Data in accordance with this EULA.

16. **Third-Party Materials & Open Source.** Certain components of the SaaS may incorporate open-source software ("**OSS**"). To the extent required by licenses covering OSS, such licenses may apply to OSS in lieu of this EULA. If an OSS license requires Honeywell to make an offer to provide source code or related information in connection with that OSS, such offer is hereby made. Honeywell may provide third party materials, including software, in connection with the SaaS ("**Third Party Materials**") which may be governed by different terms ("**Third Party Terms**"). If there are no Third Party Terms, User's use will be (a) subject to the same terms as the SaaS and (b) solely in connection with User's use of such SaaS. User is solely responsible for determining, obtaining and complying with all Third Party Terms. Honeywell has no responsibility for, and makes no representations or warranties, regarding (i) any Third Party Materials or User's use of Third Party Materials, and (ii) Third Party Terms or User's compliance with Third Party Terms.

17. **Compliance.**

a. User and its Affiliates will comply with all laws and regulations applicable to access and use of the SaaS. User acknowledges that: (a) Honeywell does not provide legal advice regarding compliance with laws and regulations related to use of the SaaS, and (b) the SaaS has functionality that could be used in ways that do not comply with laws and regulations and User is solely responsible, and Honeywell has no liability, for User's compliance with law with respect to its use of the SaaS. To the extent User or Authorized End Users are government entities, the SaaS and all associated Documentation are "commercial computer software" and related "commercial computer software documentation" and "restricted data" provided to User under "Limited Rights" and "Restricted Rights" and only as commercial end items.

b. User, individually and on behalf of its Affiliates, represents, warrants, and agrees that: (A) it is not a "Sanctioned Person," meaning any individual or entity: (1) named on a governmental denied party or restricted list, including but not limited to: the Office of Foreign Assets Control ("**OFAC**") list of Specially Designated Nationals and Blocked Persons ("**SDN List**"), the OFAC Sectoral Sanctions Identifications List ("**SSI List**"), or any other sanctions list administered by the United States, the European Union and its Member States, the United Kingdom, Switzerland, Canada, Australia, or the United Nations ("**Sanctions Laws**"); (2) organized under the laws of, ordinarily resident in, or physically located in a jurisdiction subject to comprehensive sanctions administered by OFAC (currently, but subject to change, Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic, or Luhansk People's Republic regions) ("**Sanctioned Jurisdictions**"); (3) controlled or owned, directly or indirectly, 50% or more in the aggregate by one or more of any of the foregoing; and/or (4) organized under the laws of, ordinarily resident in, or located in an unauthorized jurisdiction, including Russia; Belarus; and the Zaporizhzhia and Kherson regions ("**Unauthorized Jurisdictions**"); (B) relating to the utilization of Honeywell products, software, services, proprietary information, and technology, both Parties will comply with all Sanctions Laws. User will not, directly or indirectly, sell, export, re-export, divert, use, or otherwise transfer any Honeywell products, technology, software, or proprietary information: (i) to or for any **Sanctioned Persons**; or to, for, or involving Sanctioned Jurisdictions, Russia, or Belarus; or (ii) for any other purposes prohibited by any Sanctions Laws. User will not permit any Sanctioned Person to directly or indirectly access, use or benefit from the SaaS, or engage in or facilitate activities directly or indirectly related to end-uses restricted by Sanctions Laws. User will not source any components, technology, software, or data from any Sanctioned Persons, Sanctioned Jurisdictions or Unauthorized Jurisdictions in contravention of any Sanctions Laws. To the extent applicable, User agrees to comply with any government authorization under Sanctions Laws, including any authorization issued by OFAC in all activities involving Honeywell products, technology, software, or proprietary information. Specifically, User agrees not to remove, extract, disassemble, or otherwise disassociate any Honeywell products, technology, software, or proprietary information and store, sell, export, re-export, divert, or otherwise transfer any Honeywell products, technology, software or proprietary information in, within, from, or to a Sanctioned or Unauthorized Jurisdiction; (C) User is responsible for conducting on-going screening and monitoring and ensuring all customers and end users or other involved third parties are not Sanctioned Persons and that Honeywell products, software, technology, services, or proprietary information will not be used in, on behalf of, or for the benefit of any Sanctioned or Unauthorized Jurisdictions, including by customers or end users further down the commercial chain, as applicable. User is responsible for flowing down the obligations of this clause to all end users and/or other involved third parties, as applicable; and (D) the Parties' failure to comply with this provision will be deemed a material breach

of the transaction(s), contract(s), purchase order(s) and/or agreement(s) executed between the Parties. Each Party will notify the other Party if it violates, or reasonably believes that it will violate, any terms of this clause. The Parties may take all actions required to ensure full compliance with all Sanctions Laws without the other Party incurring any liability. For purposes of this EULA, "**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.

c. Each Party shall comply with all applicable anti-bribery laws and regulations including but not limited to the United States Foreign Corrupt Practices Act ("**FCPA**") and the United Kingdom Bribery Act of 2010. The Parties represent and warrant that they are currently in compliance with anti-corruption and anti-bribery laws and will remain so and that they will not authorize, offer or make payments, directly or indirectly, to any government authority that may result in a breach of FCPA or established restrictions or prohibitions. User agrees to maintain accurate books and records to demonstrate compliance with the compliance requirements of this section. Honeywell, at its expense, may audit User to determine compliance with such provisions upon no less than thirty (30) days' advance written notice, and User will provide reasonable assistance to Honeywell to complete such audit. User's failure to comply with this provision will be deemed a material breach of this EULA. User will not submit to the SaaS any data subject to ITAR or other Sanctions Laws.
d. Honeywell will obtain the export license when Honeywell is the exporter of record. User must obtain at its sole cost and expense all necessary import authorizations and any subsequent export or re-export license, or other approval required for the SaaS purchased, delivered, licensed or received from Honeywell. The Parties agree that technical information or technology (i.e., export-controlled information) subject to the Sanctions Laws shall not be disclosed, transferred or exported, including to any affiliate, foreign national employee, supplier, or sub-tier supplier, regardless of location, without valid export authorization or other written government approval.
e. User will notify Honeywell immediately in writing of actual or reasonably suspected violations of this section. Honeywell may suspend or terminate the EULA or the Order (or part thereof) or take other actions reasonably necessary to ensure full compliance with all laws including the Sanctions Laws without Honeywell incurring any liability.

18. **Term, Suspension.** Unless otherwise agreed in a signed writing executed by the Parties' authorized representatives, this EULA commences upon the earlier of when User's authorized representative clicks "Accept" (or similar term) or downloads/installs/accesses the SaaS and remains in effect until User ceases using the SaaS, Honeywell terminates this EULA and access to the SaaS, or User's SaaS subscription license term expires. The non-breaching Party may terminate this EULA or any Order if the other Party materially breaches and fails to cure within 30 days of receipt of written notice. Honeywell may suspend Honeywell's performance or terminate this EULA or any Order upon written notice if Honeywell believes that Honeywell's performance may violate the law and/or cause a safety or health risk, or if User is insolvent, there is an adverse change in User's creditworthiness or an attempt to obtain protection from creditors or wind down operations, User fails to pay any of Honeywell's undisputed invoices for 30 days after payment due date, User violates the law in performance of this EULA, or User assigns this EULA without Honeywell's consent. Upon termination or expiry: (a) User must pay all amounts due; and (b) if requested, return or destroy all confidential information and certify the same in writing; except for automatically generated backup copies, anonymized data or if maintained for legal purposes.

19. **Termination.** In addition to the other termination provisions of this EULA, Honeywell may terminate this EULA or any Order upon written notice if the SaaS is provided at no charge, User's use is fraudulent, or User's continued use would subject Honeywell to third party liability. Honeywell may without liability immediately suspend User's SaaS Use Rights without notice if Honeywell determines User or Authorized End Users are or may be in violation of this EULA, pose a security threat, or User's use of the SaaS is likely to cause immediate and ongoing harm to Honeywell or others. During suspension, User and Authorized End Users will not have access to the SaaS and may be unable to access Input Data (including AI Input Data). Upon termination or expiry of this EULA, User's SaaS Use Rights will expire and User must cease use of the SaaS and delete all copies of Documentation and credentials. User will remain responsible for all fees User has accrued. Within a reasonable period of time after receipt of User's request made within 30 days after the effective date of expiry or termination, Honeywell will provide a file of User's Input Data (including AI Input Data) in comma separated value (.csv) format along with attachments. Except as required by applicable law (including the Data Act), Honeywell will have no other obligation to maintain or provide to User its Input Data (including AI Input Data) and will thereafter, unless legally prohibited, delete all User's Input Data (including AI Input

Data) in its systems or otherwise in Honeywell's possession or control.

20. **EU Data Act (Switching).** This Section applies to the extent both of the following are true: (i) Regulation (EU) 2023/2854 (the "**Data Act**") applies to the SaaS provided to User under the applicable Order; and (ii) the SaaS constitutes a Data Processing Service as defined in the Data Act. For purposes of this Section, capitalized terms not otherwise defined in this EULA have the meaning given them in the Data Act. This Section prevails over any inconsistent provision of the EULA with respect to its content.

a. Switching. User may, on sixty (60) days' prior written notice, request Honeywell's assistance in porting Exportable Data to User's infrastructure or switching to an alternative provider of Data Processing Services. Honeywell will provide reasonable assistance to support switching, including providing appropriate and necessary relevant information. Honeywell will act with due care to maintain business continuity and a high level of security throughout the switching process. Switching will be completed within thirty (30) days of receiving User's request, except that Honeywell may extend the switching period by up to six (6) months if such timing is technically unfeasible. Upon written notice to Honeywell prior to the completion of switching, User may extend such switching period for a reasonable period of time.

b. Retrieval and Deletion. Upon successful completion of switching, Honeywell will retain Exportable Data for a retrieval period of at least thirty (30) days, during which time User may access such data for retrieval. Honeywell will delete Exportable Data within ninety
(90) days of conclusion of the retrieval period, unless otherwise required by applicable law or for compliance, audit, or security purposes. Honeywell will not be required to delete information held as part of regularly generated electronic backup data or archive data, the destruction of which is not reasonably practicable.

c. Termination. Upon successful completion of switching or expiry of the applicable maximum transition period, this EULA will terminate with respect to the SaaS subject to the switching request. The remainder of this EULA shall remain in full force and effect and survive such termination as to the relevant SaaS.

d. Switching Costs. Honeywell may invoice User for direct switching costs, to the extent permitted under the Data Act, for switching requests made before 12 January 2027. Nothing in this Section waives any fixed-term commitment or early-termination fees agreed in this EULA or the applicable Order. Any prepaid amounts are non-refundable, to the extent permitted under applicable law.

e. Early Termination Fee. If this EULA terminates with respect to the SaaS subject to the switching request as described herein, User shall pay an early termination fee ("**Early Termination Fee**") equal to the net present value ("**NPV**") of the remaining annual subscription fees due for the remainder of the then-current period of SaaS Use Rights stated in the applicable Order ("**SaaS Subscription Term**"), calculated from the effective date of termination through the end of the SaaS Subscription Term, using a discount rate of 9.65% per annum. User acknowledges and agrees that the Early Termination Fee is:
(i) exclusive of any direct costs associated with switching, (ii) proportionate, and (iii) solely intended to compensate Honeywell for the loss of anticipated revenue associated with early termination.

f. International Transfer. Further information on the geographic deployment of the SaaS and a general description of technical, organizational and contractual measures is available at https://www.honeywell.com/us/en/company/trust.

21. **Automatic Deactivation Feature.** User acknowledges and agrees that the SaaS may contain a time-sensitive disablement feature ("**Deactivation Device**") that will automatically deactivate the SaaS upon the termination of this EULA. User agrees not to tamper with, disable, or attempt to bypass the Deactivation Device feature. User understands that the Deactivation Device feature is integral to the enforcement of the applicable term of the license for the SaaS and agrees that Honeywell shall not be liable for any loss or damage that may arise from the disablement of the SaaS as a result of the Deactivation Device feature.

22. **Warranty & Warranty Disclaimer.**

a. EXCEPT AS EXPRESSLY STATED IN THIS EULA, THE SAAS IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. HONEYWELL IS NOT RESPONSIBLE OR LIABLE FOR USER'S (OR AUTHORIZED END USERS') USE OF THE SAAS, OR USE OR INTERPRETATION OF ITS OUTPUT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, HONEYWELL EXPRESSLY DISCLAIMS ALL CONDITIONS, WARRANTIES AND REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY REGARDING THE SAAS, INCLUDING WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY,

SATISFACTORY QUALITY AND FITNESS FOR PURPOSE. NOTWITHSTANDING THE FOREGOING, HONEYWELL MAKES NO WARRANTY THAT THE SAAS WILL MEET USER'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION OR BE ERROR FREE OR THAT ANY CYBERSECURITY SERVICES WILL PREVENT OR MITIGATE ANY ACT OR ATTEMPT TO DISRUPT, MISUSE, OR GAIN UNAUTHORIZED ACCESS TO ANY SYSTEM OR ELECTRONIC FACILITIES OR OPERATIONS THAT RESULTS IN A LOSS, ALTERATION OR DISCLOSURE OF DATA, SYSTEM DOWNTIME OR DEGRADATION OR LOSS OF OPERATION OR SERVICES RELATING TO THE CYBERSECURITY SERVICES. USER ACKNOWLEDGES THAT THE SAAS IS NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN SUCH RESULTS, DATA OR INFORMATION COULD LEAD TO PERSONAL INJURY, ILLNESS, DEATH, BUSINESS INTERRUPTION OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE.

b. HONEYWELL DISCLAIMS ALL RESPONSIBILITY AND LIABILITY FOR ISSUES, PROBLEMS, LATENCY, UNAVAILABILITY, DELAY OR SECURITY INCIDENTS ARISING FROM OR RELATED TO: (A) CONDITIONS OR EVENTS REASONABLY OUTSIDE OF HONEYWELL'S CONTROL; (B) CYBER-ATTACK; (C) PUBLIC INTERNET AND COMMUNICATIONS NETWORKS; (D) DATA, SOFTWARE, HARDWARE, SERVICES, VIRTUAL MACHINES, TELECOMMUNICATIONS, INFRASTRUCTURE OR OTHER EQUIPMENT NOT PROVIDED BY HONEYWELL, OR ACTS OR OMISSIONS OF THIRD PARTIES USER RETAINS; (E) USER'S AND AUTHORIZED END USERS' NEGLIGENCE OR FAILURE TO USE THE LATEST VERSION OR FOLLOW DOCUMENTATION;
(F) MODIFICATIONS OR ALTERATIONS NOT MADE BY HONEYWELL; (G) LOSS OR CORRUPTION OF DATA; (H) UNAUTHORIZED ACCESS VIA USER'S CREDENTIALS; (I) USER'S FAILURE TO USE COMMERCIALLY REASONABLE ADMINISTRATIVE, PHYSICAL AND TECHNICAL SAFEGUARDS TO PROTECT USER'S SYSTEMS OR DATA OR FOLLOW INDUSTRY-STANDARD SECURITY PRACTICES; OR (J) ACTS OR OMISSIONS OF USER, AUTHORIZED END USERS OR OTHER THIRD PARTIES USER RETAINS, IN BREACH OF THIS EULA.

c. THE WARRANTY DISCLAIMERS IN THIS EULA APPLY TO THE HONEYWELL AI AND FEATURES, INCLUDING ALL OUTPUTS. IN ADDITION, HONEYWELL IS NOT RESPONSIBLE OR LIABLE FOR USER'S (OR USER'S AUTHORIZED END USERS') USE OF THE HONEYWELL AI, OR USE OR INTERPRETATION OF ANY RESULTS, OUTCOMES OR OUTPUTS. HONEYWELL MAKES NO WARRANTIES REGARDING THE RESULTS OBTAINED FROM USING THE HONEYWELL AI FEATURES OR THE ACCURACY OR SUITABILITY FOR USER'S NEEDS OF ANY INFORMATION (INCLUDING, BUT NOT LIMITED TO, MATERIALS, DESIGNS, WORKFLOWS/PROCESSES, WORK INSTRUCTIONS, OR OTHER DATA) OBTAINED THROUGH THE HONEYWELL AI FEATURES, OR THAT THE HONEYWELL AI AND FEATURES WILL OPERATE IN CONJUNCTION WITH ANY OTHER PARTICULAR SAAS OR EQUIPMENT. USER UNDERSTANDS AND AGREES THAT ANY SUCH INFORMATION OBTAINED THROUGH USING THE HONEYWELL AI FEATURES IS AT USER'S SOLE RISK. USER MUST NOT RELY ON FACTUAL ASSERTIONS IN OUTPUTS WITHOUT INDEPENDENT FACT-CHECKING, AND USER MUST NOT RELY ON DESIGNS, WORKFLOWS/PROCESSES, OR WORK INSTRUCTIONS IN OUTPUTS WITHOUT INDEPENDENT REVIEW OF FUNCTIONALITY AND SUITABILITY FOR USER'S NEEDS. NO SUCH INFORMATION, SUGGESTIONS, OR OUTPUT, OBTAINED BY USER FROM THE HONEYWELL AI OR THROUGH THE HONEYWELL AI FEATURES SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN. FURTHER, USER ACKNOWLEDGES THAT HONEYWELL HAS NO OBLIGATION TO PROVIDE ANY FORM OF CYBERSECURITY OR DATA PROTECTION RELATING TO THE OPERATION OF THE HONEYWELL AI AND FEATURES. NOTWITHSTANDING THE FOREGOING, HONEYWELL MAKES NO WARRANTY THAT THE HONEYWELL AI (OR THE INFORMATION OR OUTPUT PROVIDED BY THE HONEYWELL AI) WILL MEET USER'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, BE ACCURATE, COMPLETE OR ERROR FREE OR GENERATE ANY SPECIFIC OUTCOMES OR RESULTS.

23. **Cybersecurity.** With respect to any cybersecurity-related services, software, SaaS or related hardware ("**Cybersecurity Services**"), Honeywell may provide professional judgment, technical expertise, and advice regarding User's cyber risk management program. As system performance and security are subject to multiple factors outside of Honeywell's control, Honeywell does not warrant or guarantee the Cybersecurity Services will prevent or mitigate any act or attempt to disrupt, misuse, or gain unauthorized access to any system or electronic facilities or operations that results in a loss,

alteration or disclosure of data, system downtime or degradation or loss of operation or services relating to the Cybersecurity Services (an "**Event**"). User agrees and understands that Honeywell cannot and does not, and that by working with Honeywell or using the SaaS, User may not prevent Events (either actual or attempted). User agrees and expressly acknowledges that User is responsible for its own cyber risk management program, including those responsibilities set forth in this section and in this EULA, and must participate in User's own defense and work with Honeywell to create a prioritized, flexible, repeatable, performance-based, and cost-effective process to identify, assess, and manage cyber risk throughout User's enterprise. Honeywell shall have no liability in connection with any Event unless the Event was caused by a defect in the SaaS provided by Honeywell, in which case Honeywell's sole liability and User's exclusive remedy in respect of an Event is for Honeywell to use commercially reasonable efforts to repair such defect in accordance with the Updates and Support Section of this EULA.

User represents and warrants that User will (i) use commercially reasonable administrative, physical and technical safeguards to protect User's systems, facilities, operations or data or follow industry-standard or other mutually agreed upon security practices; (ii) update to the latest version of relevant software and follow the current Documentation for the same; (iii) make no modifications or alterations to any hardware or software comprising the Cybersecurity Services without Honeywell's express written permission; (iv) designate 2 or more employees, executives, or agents (the "**Contact Person(s)**") who will respond to any Events and take recommended actions to mitigate harm to User's network; (v) develop and adopt a written governance, risk and compliance policy or policies, approved by a senior officer or User's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth User's policies and procedures for the protection of its information systems and nonpublic information stored on those information systems (the "**Cybersecurity Policy**"); (vi) develop and adopt a written incident response plan ("IRP") that is exercised and/or practiced with key scenario driven evaluations on at least an annual basis; and (vii) provide Honeywell with copies of User's Cybersecurity Policy, IRP, and business continuity or disaster recovery plans upon Honeywell's request.

24. Limitation of Liability.

a. IN NO EVENT SHALL HONEYWELL BE LIABLE UNDER THIS EULA, HOWEVER CAUSED AND REGARDLESS OF WHETHER LIABILITY ARISES FROM A BREACH OF CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), OPERATION OF LAW, OR OTHERWISE, AND EVEN IF HONEYWELL HAS BEEN ADVISED OF THE POSSIBILITY OF THE LIABILITY OR THE LIABILITY IS OTHERWISE FORESEEABLE, FOR ANY LOST PROFITS OR REVENUE, SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES OF ANY KIND (INCLUDING ALL DAMAGES DUE TO BUSINESS INTERRUPTION, LOSS OR CORRUPTION OF DATA, OR LOST USE OF ANY PROPERTY OR CAPITAL).

b. HONEYWELL SHALL HAVE NO LIABILITY FOR ANY DAMAGES OR INJURIES ARISING FROM SERVICES PROVIDED BY USER TO ITS CUSTOMERS, INCLUDING SERVICES PERFORMED BY USER USING HONEYWELL SAAS PROVIDED HEREUNDER, NOR SHALL HONEYWELL BE LIABLE FOR ANY CLAIMS OF THIRD PARTIES RELATING TO THE SAAS.

c. HONEYWELL'S AGGREGATE LIABILITY IN CONNECTION WITH THIS EULA, THE PARTIES' RELATIONSHIP, THE PROVISION OF SAAS, AND ANY PROVISION OF SERVICES TO USER, SHALL NOT EXCEED THE LESSER OF (I) THE AGGREGATE FEES PAID BY USER TO HONEYWELL FOR THE SAAS GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTHS PRIOR TO WHEN THE CLAIM AROSE AND (II) $50,000. ALL CLAIMS THAT A PARTY MAY HAVE WILL BE AGGREGATED, AND MULTIPLE CLAIMS WILL NOT ENLARGE THE FOREGOING LIMIT.

d. USER WILL NOT BRING A LEGAL OR EQUITABLE ACTION AGAINST HONEYWELL MORE THAN ONE YEAR AFTER THE FIRST EVENT GIVING RISE TO A CAUSE OF ACTION, UNLESS A SHORTER LIMITATIONS PERIOD IS PROVIDED BY APPLICABLE LAW.

e. The disclaimers, exclusions and limitations set forth herein shall apply even if any limited remedy set forth in this EULA fails of its essential purpose. The parties agree that Honeywell's prices for the SaaS provided hereunder are provided in reliance on the disclaimers, exclusions, and limitations set forth herein, and that such disclaimers, exclusions, and limitations are an agreed allocation of risk that are foundational to the bargain between the parties.

25. Governing Law and Forum.

a. The EULA is governed by the laws of the state of New York, United States of America, without regard to conflicts of

law principles. Application of the Uniform Computer Information Transactions Act and United Nations Convention on Contracts for the International Sale of Goods, 1980, and any successor law to either is specifically excluded. The parties waive any right to a trial by jury for disputes and submit to the exclusive jurisdiction of the Federal and State courts within New York State for resolution of disputes; however, Honeywell may seek an injunction or enforce a judgment against User in any jurisdiction.

b. Before the Parties initiate any dispute resolution process other than injunctive relief, the parties must schedule a mandatory executive resolution conference to be held within thirty (30) days of receipt of the other party's written request. The conference must be attended by at least one executive from each party. At the conference, each party will present its view of the dispute in detail and the executives will enter into good faith negotiations in an attempt to resolve the dispute. If the dispute is not resolved within fifteen (15) days of the end of the conference, then either party may pursue resolution of the dispute consistent with the other terms of this EULA.

26. Third Party Platforms.

a. If User accesses and uses the SaaS via a cloud-based platform (e.g., Microsoft Azure Cloud, AWS Cloud, or other cloud environment) (a "**Third Party Platform**"), this EULA is solely between Honeywell and User, and any Third Party Platform that provides access to the SaaS may have separate terms and conditions that User may be required to accept in order to access or use the SaaS. To the maximum extent permitted by applicable law, Honeywell will have no warranty, support, or other obligations whatsoever with respect to any Third Party Platform, other than to confirm whether User should be provided with access to the SaaS via such Third Party Platform. User further acknowledges and agrees that Honeywell will have no liability whatsoever with respect to any Third Party Platform.

27. Miscellaneous. This EULA and the rights granted herein are not assignable or transferable by User. Honeywell may assign or transfer this EULA or any rights in it with or without notice to User. This EULA and the Order set forth the entire agreement regarding User's use of the SaaS, superseding all prior or contemporaneous written and verbal agreements or proposals and cannot be modified except by the written agreement of both Parties. Waiver of a breach is not waiver of other or later breaches. The Parties are independent contractors of the other. If required by Honeywell's written contract with such parties, certain of its licensors may be third party beneficiaries of this EULA. The terms which by their nature are intended to survive beyond the termination or expiration of this EULA shall survive, including the Audit, Intellectual Property Rights, Data Rights, Know-how, Feedback, Indemnification, Compliance, Termination, EU Data Act (Switching), Warranty & Warranty Disclaimer, Limitation of Liability, and Governing Law and Forum Sections. The controlling version of this EULA is this English language version regardless of any 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. If any provision of this EULA is illegal or unenforceable under applicable law, the remainder of the provision will be amended to achieve as closely as possible the effect of the original term and all other provisions of this EULA will continue in full force and effect.