ONGUARD CLOUD TERMS AND CONDITIONS OF USE

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, any related mobile application ("**Mobile App**"), or hosted platform, including any updates thereto (collectively, the "**SaaS**") and related documentation ("**Documentation**") by and between the business entity using the SaaS ("**User**") and Honeywell Security Americas, LLC. 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.

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 a Mobile App, 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 Usage Metrics, Honeywell may suspend User's access until User pays all required fees to Honeywell directly or through a Provider (as defined in Section 3 below), as applicable. User or Authorized End Users may exercise SaaS Use Rights 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, personal injury, 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 Export/Import Control Laws; (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.; Further, User may not to violate the usage limits or controls set forth by: (a) the App Store Terms of Service, for iOS users accessing any Mobile App on an Apple product, or (b) Google Play Terms of Service for Android users accessing any Mobile App on an Android product. 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. "**High Risk Use**" means any uses of Honeywell AI that could or does: (i) significantly and negatively impacts Honeywell's operations or reputation; (ii) significantly and negatively impacts 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 or cause bias or discrimination; or (iii) 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) generates sexually explicit content or contravenes any regulatory safety policies; (xii) mislead any person that Honeywell AI or Outputs are solely human-generated; (xii) enter into any agreement which requires User to take any actions that are in conflict with the terms of this EULA; (xiii) sublicense, distribute or otherwise make available any portion of the Honeywell AI (including any functionality of the Honeywell AI) to any third party; (xiv) use or make any Output available to third parties without disclosing that the Output was generated using AI System.

4. **Provider Contract.** In the event the User obtains SaaS Use Rights through a Honeywell authorized third-party provider ("**Provider**"), the User hereby acknowledges and agrees as follows: a) the SaaS Use Rights are licensed on a recurring subscription basis and are subject to this EULA, together with any additional terms and conditions set forth in a separate agreement between the User and the Provider (the "**Provider Contract**"), b) Honeywell is not a party to, and bears no responsibility or liability whatsoever for, any Provider Contract, including, without limitation, any dispute arising out of or relating to (i) products or services not provided by Honeywell, (ii) User's payment obligations, (iii) any automatic renewal of the subscription term, or (iv) the termination of the User's subscription. Notwithstanding the foregoing, Honeywell shall be deemed a third-party beneficiary of the Provider Contract solely with respect to matters pertaining to this EULA and the User's compliance with its terms. The User's SaaS Use Rights are contingent upon the Provider's payment of all applicable fees to Honeywell. Honeywell shall have no liability for any loss of access to the SaaS resulting from nonpayment by either the User or the Provider, and c) unless otherwise expressly agreed by Honeywell, the User shall contact the Provider as the first line of support for the SaaS.

5. **Account.** User may be required to download an app, or visit a website, through which User accesses the SaaS and sets up accounts including issuance or authentication credentials. In operating User's account, User and Authorized End User 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 User's 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.

6. **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). NEITHER USER NOR ANY PROVIDER IS ENTITLED TO ANY DEFENSE OR INDEMNIFICATION FOR EVALUATION LICENSES GRANTED PURSUANT TO THIS SECTION.

7. **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 the 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. If User is purchasing the SaaS through a Provider, User will promptly pay the Provider the underpaid fees and related maintenance and support fees for the benefit of Honeywell.

8. **Updates & 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 SaaS Support terms, incorporated herein as Exhibit A, 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. If User is purchasing the SaaS through a Provider, User understands and agrees to contact Provider for all SaaS Support. Except 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 or third-party app 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 and reserves the right to charge additional fees for new or improved features or functionality or 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.

9. **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://hwll.co/securitypractices. 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.

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 Section 11 below). 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) and 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.** 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 ("**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.

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 by 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 the 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 Personal Data to the other Party (including providing notice).

c. 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/data-privacy. 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.

d. If Honeywell processes Personal Data on User's behalf, Honeywell's Data Processing Agreement ("**DPA**") at https://www.honeywell.com/content/dam/honeywellbt/en/documents/downloads/data-privacy/hon-honeywell-data-processing-agreement-for-customers.pdf apply.

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) User's use of the Honeywell AI for any High Risk Use or Unacceptable Risk Use; (d) User's failure to comply with this EULA, or (e) arising out of third-party claims related to Honeywell's possession, processing or use of Input Data in accordance with this EULA.

16. Cybersecurity. Honeywell may periodically conduct cybersecurity assessments on User's network systems in connection with the use of the SaaS to help identify vulnerabilities in User's network and help protect User's network. Such assessments may include, without limitation, vulnerability testing, configuration reviews, and security scans. Honeywell may, at its discretion, provide recommendations to User based on the results of these assessments, which may be subject to additional charges. User hereby acknowledges and consents to the performance of such assessments, which shall be conducted in accordance with applicable laws and regulations, and follow industry standards, including but not limited to NIST Cybersecurity Framework (CSF). With respect to any cybersecurity-related services, software, SaaS or related hardware ("**Cybersecurity Services**"), Honeywell may provide its 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 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 defective products, software or services provided by Honeywell, in which case Honeywell's sole liability and User's exclusive remedy in respect of an Event is the replacement or repair of defective products or software, or re-performance of defective services under the applicable warranty in 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 cybersecurity-related services, software, SaaS or related hardware Honeywell may provide 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.

17. **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.

18. **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 User's Authorized End User 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. User and its affiliates will comply with, and be solely responsible for compliance with, all laws and regulations on export, import, economic sanctions and antiboycott, regulated by the United States, any locality outside the United States where User conducts business, and as applicable, the United Kingdom, the European Union and its Member States, the United Nations ("**Sanctions Laws**") related to User's access to or use of the SaaS. User represents and warrants that none of User or its directors, employees, contractors, agents, banking partners, affiliates or users (a) are individuals or entities named on or acting on behalf of entities identified on applicable Sanctions Laws restricted party lists, including but not limited to, the U.S. Specially Designated Nationals and Blocked Persons List and the OFAC Sectoral Sanctions Identifications List; (b) organized under the laws of, physically located in, or ordinarily resident jurisdictions subject to comprehensive sanctions; or (c) are owned or controlled, directly or indirectly, 50% or more in the aggregate, by one or more individuals described in (a) or (b) (collectively, "**Sanctioned Persons**"). Neither User nor its affiliates will (i) permit Sanctioned Persons to directly or indirectly use, access or benefit from the SaaS, (ii) engage in or facilitate activities directly or indirectly related to any end-uses that are restricted by Sanctions Laws, or (iii) export, re-export or otherwise transfer the SaaS for any purpose prohibited by the Sanctions Laws. User will not submit to the SaaS any data subject to the U.S. International Traffic in Arms Regulations or other Sanctions Laws. User's violation of this Section will be a material breach of this EULA.

b. 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 the EULA. User will not submit to the SaaS any data subject to the Sanctions Laws.

c. 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.

d. 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.

19. 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 signs hereunder 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 3 days after payment due date, User violates the law in performance of this EULA, or 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, as defined below, and certify the same in writing; except for automatically generated backup copies, anonymized data or if maintained for legal purposes.

20. 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 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 Use Rights will expire and User must cease use of the SaaS and delete all copies of SaaS documentation and credentials. User will remain responsible for all Fees User have 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. 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.

21. EU Data Act (Switching). This Section applies to the extent Honeywell or User is subject to the Data Act and the SaaS constitutes a Data Processing Service as defined therein. 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 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 or direct switching costs permitted for switching requests made prior to 13 January 2027. Nothing in this Section waives any fixed-term commitment or early-termination fees agreed elsewhere in this EULA. Any pre-paid 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 equal to the net present value ("**NPV**") of the remaining annual subscription Fees due for the remainder of the current 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-center.

22. 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.

23. Warranty & Warranty Disclaimer.

a. EXCEPT AS EXPRESSLY STATED IN THIS EULA, THE SAAS IS PROVIDED "AS IS" AND "AS AVAILABLE" BASIS. HONEYWELL IS NOT RESPONSIBLE OR LIABLE FOR USER'S (OR AUTHORIZED USER'S) USE OF THE SAAS, OR USE OR INTERPRETATION OFF THEIR 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 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. USER ACKNOWLEDGES THAT 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 INJURY, ILLNESS, DEATH, PERSONAL INJURY, 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 USER' 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 OFF 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.

d. In the event of Honeywell's failure to conform to any applicable warranty for an iOS Mobile App, User may notify Apple, and Apple will refund the purchase price for the Mobile App, if any. Such refund, however, will be limited solely to any purchase price paid to Apple for the Mobile App. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, APPLE WILL HAVE NO OTHER WARRANTY OBLIGATION WHATSOEVER WITH RESPECT TO (A) THE MOBILE APP, AND (B) ANY OTHER CLAIMS, LOSSES, LIABILITIES, DAMAGES, COSTS, OR EXPENSES ATTRIBUTABLE TO ANY FAILURE TO CONFORM TO ANY WARRANTY. For Android Mobile Apps, GOOGLE EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY

KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

24. **Limitation of Liability.** EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS EULA OR FOR USER'S PAYMENT OBLIGATIONS, NEITHER PARTY WILL BE LIABLE FOR (A) LOST PROFITS, REVENUES, GOODWILL, OPPORTUNITY OR ANTICIPATED SAVINGS, LOSS OR CORRUPTION OF DATA OR LOSS OF USE OF PROPERTY; OR (B) INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THIS EULA. EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS EULA OR FOR USER'S PAYMENT OBLIGATIONS OR FOR EXCLUSIONS (AS DEFINED BELOW), EACH PARTY'S CUMULATIVE AND AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS EULA WILL BE LIMITED TO DIRECT DAMAGES IN AN AMOUNT EQUAL TO THE GREATER OF: (A) THE TOTAL AMOUNTS PAID FOR THE SAAS THAT GAVE RISE TO LIABILITY DURING THE 6 MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE CLAIM AND (B) U.S. $50,000. ALL CLAIMS THAT A PARTY MAY HAVE WILL BE AGGREGATED, AND MULTIPLE CLAIMS WILL NOT ENLARGE THE FOREGOING LIMIT. NOTWITHSTANDING THE FOREGOING, HONEYWELL'S LIABILITY UNDER EVALUATION, BETA, OR TRIAL RIGHTS IS LIMITED TO U.S. $1,000. THE LIMITATIONS AND EXCLUSIONS WILL APPLY TO THE MAXIMUM EXTENT PERMITTED BY LAW TO ANY DAMAGES OR OTHER LIABILITY, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, AND EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THE LIABILITY OR THE LIABILITY IS OTHERWISE FORESEEABLE, AND REGARDLESS OF WHETHER THE LIMITED REMEDIES IN THIS EULA FAIL OF THEIR ESSENTIAL PURPOSE.

    "Exclusions" are: (i) a Party's fraud or wilful misconduct; (ii) a Party's breach of confidentiality obligations (except regarding Personal Data, Input Data (including AI Input Data) (if referenced in this EULA); (iii) Section 15 (Indemnification) and Section 18 (Compliance); (iv) infringement, misappropriation or violation by a Party, its affiliates or its or their users of the other Party's or its affiliates' intellectual property rights; or (v) breach by User of any SaaS license, use rights , acceptable use terms or AI use restrictions.

    All claims and causes of action must be brought by User within 12 months of actual or constructive knowledge.

25. **Payment and Taxes**. Payment of all invoices are due within thirty (30) days of the invoice date, unless a shorter time period is specified on the invoice or otherwise communicated to the User in writing. Payments must be in accordance with the "Remit To" field on each invoice. Disputes as to invoices must be accompanied by detailed supporting information and are deemed waived fifteen (15) calendar days following receipt of the invoice. Honeywell reserves the right to correct any inaccurate invoices. Pricing excludes all taxes (including but not limited to sales, use, excise, value-added, and other similar taxes or fees imposed on the sale or transfer of goods or provision of services under this agreement), tariffs and duties, or bill of material thereof under any Trade Act, including, but not limited to, the Trade Expansion Act, section 232 and the Trade Act of 1974, section 301), and charges (collectively "**Taxes**"). User will pay all Taxes resulting from this EULA or Honeywell's performance under this EULA, whether imposed, levied, collected, withheld, or assessed now or later. If Honeywell is required to impose, levy, collect, withhold, or assess any Taxes on any transaction under this EULA, then in addition to the purchase price, Honeywell will invoice User for such Taxes unless, at the time of order placement, User furnishes Honeywell with a valid exemption certificate or other documentation sufficient to verify exemption from the Taxes, including, but not limited to, a direct pay permit.

26. **Consent to Electronic Communications and Solicitation.** To the extent the SaaS requires downloading a Mobile App, User authorizes Honeywell to send (including via email and push notifications) information regarding the SaaS, such as: (a) notices about User's use of the SaaS (and the Mobile App, including notices of violations of use; (b) updates to the SaaS and Mobile App and new features or products; and (c) promotional information and materials regarding Honeywell's products and services. User and its Authorized End Users can review account notification settings and adjust messaging preferences, including opting-in to additional messages or unsubscribing to certain messaging through the "Push Notifications" section of the Mobile App settings.

27. **Confidentiality**. Each Party may provide the other Party with certain information during the performance or fulfilment of this EULA that is not generally known, including financial information, trade secrets, know how, product data, samples, techniques, specifications, drawings, designs, design concepts, processes and testing methodologies (**"Confidential Information"**). All Confidential Information provided in connection with this EULA shall remain the property of the disclosing Party, shall be used only for the purpose of furthering the matters contemplated by this Agreement and shall be protected as confidential by the receiving Party using the same degree of care as it uses to protect its own confidential information of a similar type, but no less than a reasonable degree of care, for a period of three (3) years following the date of disclosure. These obligations shall not apply to business contact information or other information which is: (a) publicly known at the time of disclosure or becomes publicly known through no fault of receiving Party, (b) already known to receiving Party at the time of disclosure through no wrongful act of receiving Party, (c) received from a third party without restrictions similar to those in this Section, or (d) independently developed by receiving Party. Receiving Party may not disclose Confidential Information without the prior written consent of the disclosing Party, provided, however, that the receiving Party may disclose Confidential Information (i) to its affiliates, employees, officers, consultants, agents, and contractors for the purposes of discharging this EULA and complying with its legal obligations, and (ii) in response to a court order, government request, or other legally required request where, to the extent legally permitted, it (A) provides disclosing Party with sufficient notice and an opportunity to object to such disclosure (where possible) and (B) makes the disclosure subject to a protective order or other similar confidentiality restrictions. After termination or expiration of this EULA and upon written request of disclosing Party, receiving Party will return or destroy all Confidential Information and all copies

thereof, except for any Confidential Information that exists only as part of regularly generated electronic backup data or archive data, the destruction of which is not reasonably practicable.

28. **Governing Law.** The Parties agree that the following governing law shall apply: All questions or disputes arising out of or relating to this EULA and its interpretation or enforcement (including its, breach, validity and termination), and the Parties' relationship, rights, and liabilities relating hereto, whether arising in contract or otherwise ("**Dispute**"), shall be governed by the laws of the State of North Carolina without giving effect to any choice or conflict of law provisions or rule (whether the State of North Carolina or any other jurisdiction) that would cause the application of the laws of any jurisdiction other than the State of North Carolina. Honeywell and User expressly agree to exclude from this EULA the Uniform Computer Information Transactions Act and the United Nations Convention on Contracts for the International Sale of Goods, 1980, and any successor thereto. The Parties agree that the federal and state courts of Mecklenburg County, North Carolina shall be the sole and exclusive venue for any Dispute, and the Parties hereby consent and submit to the jurisdiction for such venue. The Parties irrevocably and unconditionally waive any objection to venue of any Dispute in such court and irrevocably waive and agree not to plead or claim in any such court that any Dispute has been brought in an inconvenient forum. The Parties agree that any Dispute proceeding in state court shall be litigated in the North Carolina Business Court in Charlotte, North Carolina to the fullest extent permitted by law. The Parties shall seek to designate any Dispute to the North Carolina Business Court as a complex business case under § 7A-45.4 of the North Carolina General Statutes and/or an exceptional case under Rule 2.1 of the North Carolina General Rules of Practice, and they hereby provide their consent to and agree not to contest designation to such court. If designation to the North Carolina Business Court is denied or otherwise prohibited by law, the Parties agree that any Dispute shall be litigated in Mecklenburg County Superior Court or the U.S. District Court for the Western District of North Carolina. User will not bring a legal or equitable action more than one year after the cause of action arose unless a shorter period is provided by applicable law. EACH PARTY EXPRESSLY WAIVES ANY RIGHT TO A TRIAL BY JURY RELATED TO THIS EULA.

29. **Third Party Platforms; Third Party Beneficiaries.**

a. If User accesses and uses the SaaS via a Mobile App from a third-party app store (e.g., Apple, Samsung, or otherwise) or a via a cloud-based platform (e.g., Microsoft Azure Cloud, AWS Cloud, or other cloud environment) (each, a "Third Party Platform"), this EULA is solely between Honeywell and User, and any Third-Party Platform that provides access to the SaaS or Mobile App may have separate terms and conditions to which User may be required to accept in order to access use the Mobile App. 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.

b. If User accesses and uses the SaaS via a Mobile App on an Apple device (e.g., iPhone, iPad, iPod Touch) (any such device, an "**Apple Device**"), this EULA is solely between Honeywell and User, and Apple is neither a party to this EULA nor responsible for the SaaS or any support thereof. To the maximum extent permitted by applicable law, Apple will not be responsible for the investigation, defense, settlement or discharge of any third-party intellectual property infringement claim related to the SaaS, the Mobile App, or the use thereof. User acknowledges and agrees that Apple, and Apple's subsidiaries, are third party beneficiaries of this EULA, and that, upon User's acceptance of the terms and conditions of this EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce this EULA against User as a third-party beneficiary.

c. If User accesses and uses the SaaS via a Mobile App, such Mobile App is only available for supported devices and might not work on every device. Determining whether User or its Authorized End User's device is a supported or compatible device for use of the Mobile App is solely User's responsibility, and downloading the Mobile App is done at User's or its Authorized End User's own risk. Honeywell does not represent or warrant that the Mobile App and any device are compatible or that the Mobile App will work on any device.

30. **SaaS Offering Specific Terms.** User's use of the SaaS is subject to the SaaS Offering Specific Terms at: hwll.co/EULA.

31. **Miscellaneous.** This EULA and the rights granted herein are not assignable or transferrable 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 sets forth the entire agreement regarding the 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. Unenforceable provisions will be reformed to permit enforceability with maximum effect to the original intent. Waiver of a breach is not waiver of other or later breaches. The Parties are independent contractors of the other. If required by 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. The controlling version of this EULA is this English language version regardless translation. The word "including" is exemplary meaning "including without limitation" or "including, but not limited to." The words "shall," "will," and "must" are obligatory while "may" is permissive, giving a right, but not obligation. 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. All notices, authorizations, and requests in connection with this EULA must be in writing and will be deemed delivered upon receipt at the following locations: (a) To Honeywell: Honeywell Security Americas LLC, 1212 Pittsford Victor Road, Pittsford, NY 14534, Attn: Legal Department; (b) To User: to the User's address set forth in its System Purchase Form.

WHEREFORE, for good and valuable consideration, sufficiency of which is hereby acknowledged, the Parties' authorized representatives have caused this EULA to be executed.

NAME OF USER	**HONEYWELL SECURITY AMERICAS, LLC**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT A

SaaS SUPPORT TERMS

Service Operations – Tech Support Group (TSG)

Severity 1 [Critical Priority]	**Severity 2** [High Priority]	**Severity 3** [Normal Priority]	**Severity 4** [Low Priority]	**Severity 5** [Non-Urgent Changes]
The OnGuard application is not available, which results in a **critical impact to business operations without a viable workaround**.	A feature or function of the OnGuard application is not available, which results in **intermittent service interruption or degradation impacting significant aspects of business operations** but has a viable workaround.	**Impact to the business**, however Security is not impacted.	How-to questions, minor functionality limitations, cosmetic issues, or documentation errors	Enhancement requests for product features and documentation improvements.
1-hour Response Time (phone/email contact)	1-hour Response Time (phone/email contact)	24-hour Response Time (phone/email contact)	24-hour Response Time (phone/email contact)	48-hour Response Time (phone/email contact)

Service Operations – Cloud Ops Engineering (COE)

Severity 1 [Critical Priority]	**Severity 2** [High Priority]	**Severity 3** [Normal Priority]	**Severity 4** [Low Priority]	**Severity 5** [Non-Urgent Changes]
Servers unavailable, i.e., hard-down/offline due to infrastructure failure, which **critical impact to business operations without a viable workaround.**	Part of the system is unavailable or malfunctioning due to infrastructure failure, which **intermittent service interruption or degradation impacting significant aspects of business operations** but has a viable workaround.	**Impact to AWS Infrastructure,** ie a server needs to be re-built; however, Security is not impacted.	How-to questions, billing data inquiries (ie customer has concerns around cost overruns and wants to know more about their usage)	Enhancement requests to infrastructure, ie adding a new region, or a new Open Access API integration that isn't working right.
1/2-hour Response Time (phone/email contact) 6-hour Targeted Resolution Time	1-hour Response Time (phone/email contact) 12-hour Targeted Resolution Time	12-hour Response Time (phone/email contact) 24-hour Target Resolve Time	24-hour Response Time (phone/email contact) 48-hour Target Resolve Time	72-hour Response Time (phone/email contact)