

CYBERSECURITY TERMS

1. Agreement. The specific cybersecurity software, software-as-a-service, hardware and/or service offerings for which you have contracted (the “**Cybersecurity Products**”) will be identified in a print or electronic document identified as a “proposal”, “order”, “agreement” or similar name (the “**Order Form(s)**”). Order Forms identify each transaction’s contracting entities, pricing and related provisions and may reference or link to supplemental terms, agreements or policies and references to Order Forms includes such documents. The Order Form together with these Cybersecurity Terms and all other terms, conditions, and documents expressly referenced therein form a single contract (the “Agreement”). Notwithstanding any other terms of the Agreement, these Cybersecurity Terms take precedence over any other terms in the Agreement with regards to the Cybersecurity Products and any conflicts shall be resolved in favor of these Cybersecurity Terms.

2. Parties. “**Honeywell**”, “**we**”, “**us**” or “**our**” means Honeywell International Inc. or Affiliate(s) who execute or assent to the Order Form. “**You**” or “**your**” means collectively the other entities executing or assenting to the Order Form. “**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.

3. Shared Responsibility, Remedy, and Warranties. You acknowledge and agree that Honeywell provides professional judgment, technical expertise, and advice to you regarding your cyber risk management program. You acknowledge and agree that you recognize your own responsibility (as further detailed below in 3.B. of this Agreement) with respect to your cyber risk management program and that Honeywell provides highly integrated Cybersecurity Products to you. As ultimate system performance and security are subject to multiple factors outside of our control, we do not warrant or guarantee the Cybersecurity Products will prevent or mitigate every Event (as defined below). You agree and understand that we cannot and do not prevent Events (either actual or attempted), or, that by working with us, you will not experience such actual or attempted Events. Instead, you agree and expressly acknowledge that you must participate in your own defense and work with us to create a prioritized, flexible, repeatable, performance-based, and cost-effective approach to establish an ongoing process to identify, assess, and manage cyber risk throughout your enterprise. Though this Agreement specifies certain responsibilities that you must accept, any such list should not be considered absolute. **Our sole liability and your exclusive remedy in respect of an Event is: (a) if the Event was caused by defective products or services provided by us, replacement or repair of defective products, or re-performance of defective services under the applicable warranty in the Agreement.** An “**Event**” means 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 Products.

A. Honeywell’s Representations and Warranties. Honeywell represents and warrants (i) that it will perform the Cybersecurity Products using personnel of required skill, experience and qualifications in a professional manner leveraging generally recognized industry standards for similar services and will devote adequate resources to meet its obligations under this Schedule; and (ii) that the Cybersecurity Products will be made available and performed on a professional, reasonable efforts basis. Honeywell makes no guarantees regarding the effectiveness of the Cybersecurity Products with respect to your overall cybersecurity program due to Honeywell’s lack of control over numerous aspects of your operations, personnel, and Information Systems. Honeywell is thus not responsible or liable for any issues, problems, unavailability, delay, or Events arising from or related to: (i) force majeure events as described below; (ii) the public internet and communications networks; (iii) data, software, hardware, services, telecommunications, infrastructure, or networking equipment not provided by us or acts or omissions of third parties you retain; (iv) your negligence or failure to use the latest version or follow published documentation; (v) modifications or alterations not made by us or services we do not perform; (vi) breach, loss or corruption of data; (vii) unauthorized access via your credentials; or (viii) your failure to use commercially reasonable administrative, physical and technical safeguards to protect your systems, facilities, operations or data or follow industry-standard or other mutually agreed upon security practices.

B. Your Representations and Warranties. You represent and warrant that you will (i) use commercially reasonable administrative, physical and technical safeguards to protect your 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 Products without our express written permission; (iv) designate two (2) or more employees, executives, or agents (the “**Contact Person(s)**”) who you guarantee will respond to any Events and take recommended actions to mitigate harm to your network; (v) develop and adopt a written governance, risk and compliance policy or policies, approved by a senior officer or your board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth your 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 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 us with copies of your Cybersecurity Policy, IRP, and business continuity or disaster recovery plans upon our request. You and your personnel (and not Honeywell) are responsible for maintaining the confidentiality of, and all use of, and actions taken using any passwords and access rights assigned to You or your personnel in connection with any of the Cybersecurity Products.

4. Third-Party Products. To the extent that we provide third-party products, software, hardware or services (“**Third-Party Products**”) in relation to the Cybersecurity Products, then notwithstanding any other terms agreed to between us, you agree that all Third-Party Products are provided subject to the Third-Party Product supplier’s terms and conditions (including any applicable software license terms) in effect at the time such Third-Party Products are delivered to you. We have no liability with respect to the performance or non-performance of such Third-Party Products, including but not limited to any liability arising out of any Events caused by defects or failures of such Third Party Products.

5. Licenses. We may use open-source software (“**OSS**”) and to the extent required by the licenses covering OSS, the terms of such licenses will apply to OSS in lieu of this Agreement. To the extent the licenses applicable to OSS: (i) prohibit any restriction with respect to such OSS, such restriction will not apply to such OSS; and (ii) require us to make an offer to provide source code or related information in connection with the OSS, such offer is hereby made. If required by our written contract with them, certain of our licensors are third-party beneficiaries of the Agreement.

6. Limitation of Liability. WITH RESPECT TO ALL CYBERSECURITY PRODUCTS AND EVENTS, WE ARE NOT LIABLE FOR INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS AND REVENUES. OUR CUMULATIVE AND AGGREGATE LIABILITY TO YOU WITH RESPECT TO ALL CYBERSECURITY PRODUCTS AND ANY CYBERSECURITY EVENT IS LIMITED TO DIRECT DAMAGES IN AN AMOUNT NOT TO EXCEED THE AMOUNTS PAID BY YOU FOR THE CYBERSECURITY PRODUCTS IN QUESTION. OUR LIABILITY UNDER AN EVALUATION OR TRIAL IS LIMITED TO USD \$1,000. THE LIMITATIONS AND EXCLUSIONS APPLY TO ALL CLAIMS AND CAUSES OF ACTION ARISING OUT OF OR IN RELATION TO THE CYBERSECURITY PRODUCTS GOVERNED BY THE AGREEMENT REGARDLESS OF FORM. THIS CAP SHALL APPLY TO A BREACH OF YOUR CONFIDENTIAL INFORMATION CAUSED BY LOSS, CORRUPTION, OR ACCESS TO YOUR DATA. IN NO EVENT SHALL HONEYWELL BE LIABLE OR RESPONSIBLE FOR LOSS OF OR DAMAGE TO YOUR DATA OR RECORDS.

7. Force Majeure. Honeywell shall not be liable or responsible to you, nor be deemed to have defaulted or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement when and to the extent such failure or delay is caused by or results from acts or circumstances beyond Honeywell’s reasonable control including, without limitation, acts of God, flood, fire, earthquake, explosion, governmental actions, war, invasion or hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest, national emergency, revolution, insurrection, epidemic, lock-outs, strikes or other labor disputes (whether or not relating to either party’s workforce), or restraints or delays affecting carriers or inability or delay in obtaining supplies of adequate or suitable materials, materials or telecommunication breakdown or power outage, provided that, if the event in question continues for a continuous period in excess of 60 days, Customer shall be entitled to give notice in writing to Honeywell to terminate this Agreement.

8. Miscellaneous. Any additions or changes to these Cyber Products Terms must be in the form of a mutually agreed document signed by both parties. We have the right to analyze, transfer (including outside of your territory or country), and otherwise use your data to provide, improve and develop our cyber security Services. For Cybersecurity Products sold on a subscription or periodic basis, the Agreement commences on the effective date of, and continues for the duration in the Order Form. Upon termination or expiry, you must pay all amounts due under the Order Form. Your purchase orders are identified only to authorize payment and any terms or conditions in any purchase order are not a part of the Agreement or controlling.