**CYBERSECURITY TERMS**

**1. Cybersecurity Terms**. These cybersecurity terms (the "Cybersecurity **Terms**") set out the terms and conditions applicable to any cybersecurity-related Services, software, SaaS or related hardware ("**Cybersecurity Services**") identified in the Order Form and form part of the Agreement. The Cybersecurity Terms take precedence over other Agreement terms in relation to the Cybersecurity Sevices.

**2. Events**. With respect to any Cybersecurity Services, Honeywell may provide professional judgment, technical expertise, and advice regarding Buyer'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**"). Buyer agrees and understands that Honeywell cannot and does not, and that by working with Honeywell or using Offerings, Buyer may not prevent Events (either actual or attempted). Buyer agrees and expressly acknowledges that Buyer is responsible for its own cyber risk management program, including those responsibilities set forth in this section and in this Agreement, and must participate in Buyer'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 Buyer'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 Buyer'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 Agreement.

**3. Buyer Responsibilities**: Buyer represents and warrants that Buyer will (i) use commercially reasonable administrative, physical and technical safeguards to protect Buyer'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 Buyer's network; (v) develop and adopt a written governance, risk and compliance policy or policies, approved by a senior officer or Buyer's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth Buyer's policies and procedures for the protection of its information systems and nonpublic information stored on those information systems (the "**Cybersecurity Policy"**); and (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.