Honeywell Forge Performance+ for Buildings Offering Descriptions and Terms

Version: 3.0

These offering specific terms listed below ("**Offering Terms**") set out the terms and conditions applicable to the Honeywell Forge for Building Performance+ offerings ("**SaaS**") made available by Honeywell as identified in the print or electronic document identified as "proposal", "order", "agreement" or similar name ("**Order**"). Access and use of the SaaS is governed by these Offering Terms, the Order and the applicable End User License Agreement ("**EULA**") available at hwll.co/eula (together, the "**Agreement**"). All terms not defined herein have the meaning given to them in the Agreement. In the event of any conflict or inconsistency among the terms of the following documents, the order of precedence shall be as follows: 1) these Offering Terms, 2) the EULA, 3) the Order. Honeywell may update these Offering Terms from time to time. Honeywell will make commercially reasonable efforts to notify User of any material changes. Continued use of the SaaS constitutes User's consent and agreement to such changes.

A. Offering Descriptions

Product	Description
Honeywell Forge Performance+ for Buildings | Predictive Maintenance	The Predictive Maintenance Software-as-a-Service ("**SaaS**") solution enables selected asset insights for User's building operations and is designed to help reduce operational and maintenance costs and to improve occupant comfort, asset availability and sustainability of User's building portfolio. The Predictive Maintenance Offering features available are stated below. The specific features for User will be set forth in the Order. • Analytics • Centralized Control • Alert Management • iOS Mobile App • Asset Reliability

B. Offering Package and Feature Descriptions

Product Features	Description
Analytics	The Analytics feature continuously inspects the building operation and identifies issues and anomalies in the operations. The early detection and notification of problems enables the service technician to reduce the "search" time and to fix the issue, minimizing the impact on energy, comfort, or asset availability. The Analytics feature gives the User near real-time visibility of the comfort performance level of its building and rule-based generation of service cases. This feature may include advanced analytics leveraging Artificial Intelligence (AI) and Machine Learning (ML) algorithms, including generative AI capabilities, based on building characteristics, to continuously inspect building operations, such as HVAC anomalies. AI and ML models may supplement rules-based method for fault prediction by forecasting trends of equipment degradation, anomaly detection by identifying observations within the data that are different from the majority, and root cause analysis which provides explanations on the likely reasons for observed abnormalities in the asset. These advanced algorithms provide insights into data and may automatically learn and adapt to changes. Always validate the accuracy of the insights by referring to the source information directly.
Centralized Control	Centralized Control provides Authorized End Users with the ability to review the performance of assets and triage issues by providing historical trend data and near-real-time site data, and the ability to control HVAC equipment to resolve remotely issues across their site or portfolio directly from Honeywell Forge portal. By enabling Centralized Control through Honeywell Forge Performance+, Users have the ability to control their building remotely which may reduce the need for onsite visits

	and help reduce unnecessary travel and maintenance costs. Certain control functionality may only be available for some deployment topologies. *The User is responsible for confirming and ensuring all on-site personnel and system safeguards are maintained when servicing and supporting site equipment recommended for triage through Centralized Control.
iOS Mobile App	The Mobile App is only available at this time in iOS. The Mobile App is designed for Authorized End Users from facility managers to technicians and provides access to core functionality of Predictive Maintenance and Centralized Control on iOS mobile phones. Authorized End Users can view KPIs for their sites.
Alert Management	This functionality allows Authorized End Users to view and manage alarms generated in connected on-premises systems in the Honeywell Forge portal. Authorized End Users will be able to view alarms, including their status, from across their portfolio of buildings, to triage alarms using Centralized Control (if Authorized End Users has that option), to acknowledge alarms and, if required, to create a service case within Honeywell Forge portal which can be assigned to relevant teams alongside the service cases that come from Honeywell Forge analytics.
Asset Reliability*	The Asset Reliability feature is a SaaS solution that provides asset health monitoring, fault diagnosis and failure prediction for rotating equipment using wireless vibration sensors that link to a cloud solution with analytics, an intuitive user interface and integrated alerting system. User acknowledges and understands that this feature relies on certain hardware (Hardware) as pre-requisite which is not included in the price for the SaaS subscription and must be purchased separately. The additional fees for such Hardware are set forth in the Order. *This feature is only available in the United States, Canada, the European Union, Switzerland, the United Kingdom, India, Australia, New Zealand, South Africa, and the UAE.

C. General Offering Terms

1. **Gateway**. As a part of the SaaS, Honeywell will provide User with certain hardware and/or software to install and run on User's Site which will facilitate the information transfer to and from User's Sites and the Honeywell Forge Cloud (collectively **"Honeywell Forge Connect Software"** and/or **"HFCS"**). In regard to HFCS, Honeywell grants User a limited, revocable, non-exclusive, non-assignable, non-transferable license to certain software components, as managed and secured in User's hosting environment, that User will need to install, promptly update or allow Honeywell to update (when applicable). This software will be provided solely for the purpose of using Gateway (defined below) at Sites. Honeywell Forge Cloud is the cloud environment maintained by Honeywell to operate the SaaS. Unless Honeywell provides you with hardware as detailed in the Order, User will provide a virtual machine/hardware with an operating system (**"HFCS Execution System")** in a certified configuration, as specified by Honeywell, which will host the HFCS. HFCS as provided by Honeywell and the HFCS Execution System collectively forms a Honeywell Forge Connect Gateway (also referred to as **"Gateway")**. Depending upon User's unique demands as to performance, availability, throughput, and other requirements, User may require multiple Gateways in its environment. Honeywell, its affiliates, licensors and suppliers own all intellectual property rights in the provided HFCS and Offerings, and reserve all rights not expressly granted to User under this Order. User shall, promptly notify Honeywell of any known security breach that impacts the Gateway. Upon termination of User's subscription of the SaaS, User will delete the HFCS from all Gateways in use and/or return any hardware provided by Honeywell (when applicable), in the manner as mutually agreed between the parties.

   User acknowledges and agrees that User will be responsible for ensuring that the Gateway is properly and adequately secured and protected. To facilitate communication to the Gateway, User will need to provide adequate network connectivity to allow access to User's data sources. Providing network connectivity may include providing internet connection, sharing proxy configurations, configuring certificates, opening ports and updating firewall rules, etc. User is responsible for compliance with applicable laws implicated by use of the Gateway and for maintaining User's equipment and infrastructure to meet the required security, performance, availability, and other connectivity related criteria to use the SaaS. Honeywell will provide materials with the HFCS which should enable User to independently configure and install the Gateways. User will also find contact details for technical support included in the materials.

2. **Gateways Updates**:

   a) **Honeywell-Provided HFCS Execution System**. Honeywell may periodically update (remote and/or on-premise) the HFCS Execution Systems and/or the HFCS. Honeywell may provide notice in regard to the updates for the HFCS

Execution Systems and/or the HFCS and the time duration within which the updates should be applied by User. Users agree to provide all necessary support for these updates. In the event User requires Honeywell assistance with updating or troubleshooting the HFCS Execution System and/or HFCS, User will need to grant Honeywell remote access. Such work is subject to additional fees.

b) **User-Provided HFCS Execution System.** Honeywell may periodically need the HFCS Execution Systems to be updated. Honeywell will publish information about the required updates for the HFCS Execution Systems and the time duration within which the updates should be applied by User. User understands and acknowledges that the virtual machine/hardware associated with the HFCS Execution Systems may need to be replaced from time to time and that this is User's responsibility and at User's cost. In the event User requires assistance from Honeywell with updating or troubleshooting the HFCS Execution System, User will need to grant Honeywell remote access. Such work is subject to additional fees. Honeywell will not be liable for the damages or losses caused by User's failure to timely update or secure the Gateways. From time to time, Honeywell may push and/or update the HFCS.

3. **Third-Party Systems**. Honeywell does not provide support for or guarantee interoperability with third-party systems, and Honeywell is not responsible for the integrity, availability, or quality of data provided by third-party systems. User is solely responsible for providing or updating any dependent third-party components and making sure its use of the SaaS is in conformance with any applicable third-party requirements, including service and/or warranty requirements.

4. **User Responsibilities:**

a) User agrees that it shall maintain all minimum requirements in order to use the SaaS as provided by Honeywell, which includes but is not limited to maintaining an online Forge Connect Gateway as deployed. Such minimum requirements may be updated from time to time.

b) The SaaS may require firewall rule configurations made on the User's premises. These include northbound firewall configurations for data sent to/from the Forge Cloud, including machine data transmitted to the cloud, lifecycle management configuration data sent back to the device, and edge software updates. Certain features and functionality of the SaaS may allow User to enter its own analytics or set points, dashboard and/or configurations. Any default analytics and set points provided in the SaaS are intended to help inform User's decisions, but ultimately, User is responsible for any analytics and set points. User agrees not to upload, or permit the uploading of, sensitive personal data into the SaaS (including but not limited to social security numbers, bank account numbers, credit card numbers, geolocations) and industry specific sensitive or regulated data. Honeywell may provide self-service training modules to assist with the provision of SaaS training to Users. On-site training may be available at an additional fee.

c) Honeywell is not responsible for any output provided by the SaaS, or any action taken by User based on the output of the SaaS. Actions taken on output of the SaaS may be visible to all Authorized End Users and applicable across the entire Site. The SaaS is not intended for, or to meet, any sustainability, carbon, or cyber regulatory compliance requirements. User agrees that it will not rely on the SaaS for any life safety, critical or other regulatory compliance purposes. SaaS is not designed or intended for real-time or time-critical control of User's equipment, internet and network connectivity, and infrastructure (i.e., sensors, building assets, base control system, OPC server, network switches, and IoT devices, etc.) nor for emergency situations and should not be relied upon as a primary system. Its operational use is limited to a system for monitoring and managing equipment for general operations and maintenance insights. The SaaS is not a substitute for a third-party monitored emergency notification system. Honeywell makes no representation or warranty that use of the Offering will improve User's operations, safety, sustainability, cyber capabilities, or reliability.

D. Customer Site Readiness

In order to deploy, implement and maintain the SaaS, User will ensure that each Site meets minimum Site readiness requirements as required by the SaaS ("**Site Readiness**"). Honeywell is not liable for any delays or impairment of SaaS functionality caused by User's failure to provide and maintain Site Readiness, and User will remain responsible for all payments and obligations provided in an Order irrespective of any such delays or failures. For the Site Readiness areas identified below as "Pre-Site Connection", these readiness conditions must be met by User before any Honeywell implementation work as set forth in the Order can be undertaken. Other areas not identified as Pre-Site Connection, in addition to any other requirements provided by Honeywell, must be maintained by User as ongoing Site Readiness responsibilities during the subscription term of the SaaS. The minimum Site Readiness requirements that User will provide include, but are not limited to:

- Pre-Site Connection - As part of a Site assessments, data and documentation on Site architecture, systems, vendors,

utilities, assets and connectivity requirements;

- Pre-Site Connection - Site network, port and secure locations for installation of hardware and software;
- Pre-Site Connection - User IT team access and IT technical information to connect SaaS;
- Pre-Site Connection - Approved firewall to deny inbound and restrict outbound access to User systems;
- Pre-Site Connection - Connectivity to the internet with suitable reliability and bandwidth to uplift the projected data rates;
- Dedicated User team, including a lead project manager, an ICT/IT go to person, a Site expert, and executive sponsor, to ensure all Site Readiness requirements are met;
- Access to all Site assets and systems, and related data, such as utility meters and air handling systems, to enable the SaaS;
- Live and historical data need to be in the same format. Adopting different formats for the live and historical data feed may cause longer onboarding time;
- Up to date endpoint protection installed and configured on all servers and workstations;
- Maintenance of firewall, servers, operating systems and application patching, backups, and endpoint protection;
- Processes for change management, log review, disaster recovery, incident management, patch management, and credential management; and
- Monitoring solution shall be in place to detect missing software updates and patches

E. Asset Reliability Feature Terms

The following additional terms only apply to your purchase of the Asset Reliability feature.

1. **Hardware Installation and Maintenance:** The Hardware is designed for non-invasive installation. User is required to install and secure the Hardware, unless otherwise indicated in the Order. If User installs the Hardware, User agrees to abide by all instructions and Hardware Documentation as provided by Honeywell, including for installation and configuration. User is solely responsible for any installation issues. For Hardware sensors to adhere to User's systems, User understands that installation may require magnet, epoxy resin, or adherence to studs, as applicable to your Site. User will not identify or install sensors to any system or asset if the installation method may adversely affect or impact your Site systems or assets. User must ensure that the Hardware remains as installed during its subscription and User maintain Site protections in place to prevent tampering or interference. User is solely responsible for any costs, expenses, damages and/or repairs relating to the installation, tampering and/or removal of the Hardware.

2. **Connectivity:** The Hardware sensors provided as part of the Asset Reliability feature may come pre-installed with their own sim card which must only be used in conjunction with that specific sensor. User is not permitted to remove sim cards from sensors. Unless specified otherwise in the Order, User must use the cellular data connectivity service provided with the cellular sensors and User is not permitted to procure its own cellular service. To ensure satisfactory performance of the Asset Reliability feature User may be required to provide information about its communication network strength at the site of the Hardware installation along with network equipment details necessary to assist in any support of the Hardware. Asset Reliability depends on continuous cellular or Wi-Fi connectivity and it will not function as intended if connectivity is poor or lost. It is User's responsibility to ensure that the Site of the Hardware installation has sufficient cellular or Wi-Fi coverage to enable Asset Reliability to function properly. User acknowledges that cellular or Wi-Fi connectivity operates on radio and signal frequencies and multiple external sources can impact the quality or availability of signal transmission. Honeywell is not responsible for connectivity issues, and Honeywell gives no warranty or guarantee as to network coverage, quality or availability. Honeywell is not responsible for lost data and User agrees to implement adequate backup storage.

3. **Cellular Data Usage:** For cellular enabled sensors, the Asset Reliability feature includes data connectivity services, and the SaaS Subscription Fee includes cellular data of 30MB per month per sensor. Honeywell reserves the right to charge additional fees if the cellular data usage exceeds 30MB. Honeywell recommends that User follow the guidelines in the table immediately below to prevent data usage exceeding 30MB per month.

Machine RPM	Max uploads per day
<500	Additional data likely to be required
500-1000	Max 2
1001-1600	Max 4
1601-3000	Max 6

>3001	Max 12

4. **Batteries and Defective Hardware:** The sensor batteries typically have a battery life of approximately 3 years to 8 years. Exceeding the recommended number of uploads per day or otherwise failing to follow the Hardware Documentation may reduce the expected battery life. User is responsible for any battery replacement required. Honeywell will repair or replace, at Honeywell's own discretion, defective Hardware provided as part of the Asset Reliability feature, excluding failures resulting from tampering, abuse, damage, incorrect installation, unauthorized modification or negligence caused by User.

F. Analytics Instructions for AI-Based Summaries and Recommendations

The following instructions only apply to User's purchase of the Analytics feature.

1. **Artificial Intelligence and Machine Learning**: The AI functionality is designed to offer insights and summaries of service cases, based on historical data, leveraging pattern recognition and data analysis to aid in decision-making. The AI generates concise summaries of service cases and provides recommendations based on recognized patterns within historical data.
2. **Accuracy**: The summary responses generated by the AI functionality may not always be accurate. Outputs are AI-generated and may be inaccurate or contain errors or omissions. It is imperative that Authorized End User's validate these responses by cross-checking with the source information. For further details and to validate accuracy of AI-generated summaries, please refer to the source information directly.
3. **Usage**: Any use of the AI-generated summaries and recommendations outside of the instructed purposes is strictly prohibited and is done at the User's own risk. Follow User's company's work procedures, safety protocols, or other processes instead of (or in addition) the outputs produced by AI. For the Authorized End User's safety, it is important to note that responses may not contain all necessary safety information. Authorized End Users should carefully review product manuals and User's company requirements for maintenance and troubleshooting live equipment. If in doubt, escalate within User's company for assistance. User's use of the Honeywell AI functionality is subject to the Agreement between User and Honeywell. Please review the Agreement.