Honeywell Forge Performance+ for Buildings Offering Descriptions and Terms

Version: 2.2

The Offering terms listed below form part of your Order Form and Agreement ("**Offering Terms**"). All terms not defined have the meaning given to them in the Agreement. In the event of conflict between these Offering Terms and the Agreement, these Offering Terms will prevail. We may update these Offering Terms from time to time. We will make commercially reasonable efforts to notify you of any material changes. Continued use of the Offering(s) constitutes your consent 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 your building operations and is designed to help reduce operational and maintenance costs and to improve occupant comfort, asset availability and sustainability of your building portfolio. Predictive Maintenance Offering features available are stated below. Certain features may have additional charges, as indicated in an Order Form. • Honeywell Forge Connect Gateway • Predictive Maintenance • Centralized Control • Alert Management • iOS Mobile App • Tailored Dashboard Services ("TDS"). (Each TDS subscription license entitles Customer to 3 Users. Additional licenses and fees required for additional Users.) • Enterprise Integrations • End-to-End Extensibility Professional Services • Asset Reliability*

B. Offering Package and Feature Descriptions

Product Features	Description
Honeywell Forge Connect Gateway	An intelligent IoT Gateway which has the ability to easily connect the existing equipment and assets in a building through the device to seamlessly link the data into the Honeywell Offerings.
Predictive Maintenance	Predictive Maintenance is a data analytics service that 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. Predictive Maintenance gives you near real-time visibility of the comfort performance level of your building and rule-based generation of service cases.
Analytics, such as Artificial Intelligence (AI) & Machine Learning (ML) Models	Some of our products may include advanced analytics including AI and ML algorithms, depending 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 automatically learn and adapt to changes.
Centralized Control	Centralized Control provides 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. 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. *Customers are responsible to confirm and ensure all on-site personnel and system safeguards are maintained when servicing and supporting site equipment recommended for triage through Centralized Control.
Enterprise Integrations	Enterprise Integrations allows Customers to integrate other applications with the Honeywell Forge Buildings applications through application program interfaces ("API(s)"). APIs are provided pursuant to Honeywell DevTool terms and are solely for use by Customer. At present the only supported API is for service cases and Suite of Search as A Service API's (referred to as "Find API"); other APIs may be available in the future and API usage (including Find API) may require additional developer terms. Additionally, pre-defined or "starter" integrations with third party systems may be made available to help accelerate the integration with commonly used systems. Enterprise Integrations and any starter integrations may incur additional costs and are provided as an additional professional service.
End to End Extensibility Professional Services	End-to-End-Extensibility Professional Services includes the ability to customize the Predictive Maintenance application with new assets, rules and reports. This includes the ability to add new assets and asset types to the Predictive Maintenance application along with the creation of custom analytic rules and generation of service cases based on the rule logic. The new asset types and associated assets will be displayed in the asset availability dashboard and any generated service cases or faults would be included in the Service Cases dashboard and Fault Summary dashboard. Additional dashboards specific to these new assets can be provided by adding the Tailored Dashboard Service to the Offering.
Tailored Dashboard Service ("TDS")	*An add-on service to Predictive Maintenance that, for an additional cost, provides added UI visualization options for existing Predictive Maintenance dashboards using pre-defined and available dashboard options and widget library from Honeywell based common use cases from available sensor and asset data at Customer's site. TDS allows the flexibility to expand dashboards with additional visualizations of telemetry data already connected to the Honeywell Forge Performance+ platform. It enables you to better track asset performance and accelerate problem identification. The development and range of visualizations is performed by Honeywell support teams in direct collaboration with you and the full scope will be mutually agreed in writing after a workshop.* *Customer requirements for TDS:* • Maintain active and concurrent Predictive Maintenance Subscription, as TDS can only provide information that is processed through Predictive Maintenance. • Customer will finalize and execute TDS Scope document following execution of this Agreement. • Provide timely access to staff needed as part of dashboard workshop and troubleshooting. • Ensure that Customer complies with any and all applicable laws, filings and/or regulations in regard to the dashboards you request be displayed using TDS. TDS is also provided in reliance on certain third party features, support and tools. In provisioning and supporting TDS, Honeywell may need to engage third party services for certain levels of support. You agree to designate certain technical contacts ("Technical Contacts") that will be the primary Customer point of contact for the workshop, deployment, and assisted support of TDS. These Technical Contacts will provide first-tier assistance to support your User's questions regarding TDS and will act as the sole point of contact with respect to your purchase and use of TDS, and who will work cooperatively with us to facilitate resolution of reported TDS problems.
iOS Mobile App	The Mobile App is only available at this time in iOS. The Mobile App is designed for Users from facility managers to technicians and provides access to core functionality of Predictive Maintenance and Centralized Control on iOS mobile phones. Users can view comfort, asset availability and service case KPIs for their sites and drill down to view details of open service cases and review individual zone and asset performance in their facilities. Additionally, Users can triage service cases by reviewing asset property trends and live values and, with the necessary

	permissions, can make control changes including set points and relinquishing control.
Alert Management	This functionality allows Users to view and manage alarms generated in connected on-premises systems in the Honeywell Forge portal. Users will be able to view alarms, including their status, from across their portfolio of buildings, to triage alarms using Centralized Control (if User has that option), to acknowledge alarms and, if required, to create a service case within Honeywell Forge which can be assigned to relevant teams alongside the service cases that come from Honeywell Forge analytics. As this functionality is bundled with Centralized Control only, a User can have Centralized Control alone bundled with alerts, or Centralized Control with Predictive Maintenance without alerts; or Centralized Control with alerts and Predictive Maintenance.
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. Sensors are provided as part of the SaaS solution on a subscription basis. *Limited Availability

C. General Offering Terms

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

   The Gateways sit in your environment, and you acknowledge and agree that you are responsible for ensuring that they are properly and adequately secured and protected. To facilitate communication to the Gateway, you will need to provide adequate network connectivity to allow access to your data sources. Providing network connectivity may include providing internet connection, sharing proxy configurations, configuring certificates, opening ports and updating firewall rules, etc. If your network connectivity causes SaaS availability issues, these will not be factored into our SaaS availability calculation. You are responsible for compliance with applicable laws implicated by your use of the Gateway and for maintaining your equipment and infrastructure to meet the required security, performance, availability, and other connectivity related criteria to use the SaaS. You agree to only use and locate the Gateways at the site addresses listed in the Order Form. We will provide materials with the HFCS which should enable you to independently configure and install the Gateways. Included in the materials you will also find contact details for technical support.

2. **Gateways Updates**: A. **Honeywell-Provided HFCS Execution System**. We may periodically update (remote and/or on-premise) the HFCS Execution Systems and/or the HFCS. When able, we will provide notice in regard to the updates for the HFCS Execution Systems and/or the HFCS and the time duration within which the updates will be applied by you. You agree to provide all necessary support for these updates. In the event you require our assistance with updating or troubleshooting the HFCS Execution System and/or HFCS, you will need to grant us remote access. B. **Customer-Provided HFCS Execution System**. We may periodically need the HFCS Execution Systems to be updated. We will publish information about the required updates for the HFCS Execution Systems and the time duration within which the updates need to be applied by you. You understand and acknowledge that the virtual machine/hardware associated with the HFCS Execution Systems may need to be replaced from time to time and that this is your responsibility and at your cost. In the event you require our assistance with updating or troubleshooting the HFCS Execution System, you

will need to grant us remote access. We will not be liable for your failure to timely update or secure the Gateways. From time to time, we may push and/or update the HFCS.

3. **Third-Party Systems**. We do not provide support for or guarantee interoperability with third-party systems, and we are not responsible for the integrity, availability, or quality of data provided by third-party systems. Please note that you are responsible for providing or updating any dependent third-party components.

4. **Customer Responsibilities: A**. Customer agrees that it shall meet all minimum requirements for the Offering(s) which are provided by Honeywell with the Agreement, which will include maintaining an online Forge Connect Gateway as deployed. Such minimum requirements may be updated from time to time. **B**. The Offering(s) provide you with information about equipment health, equipment performance, operation metrics and business metrics to help inform your decisions around equipment and operations which may include machine downtime, maintenance activities, operation bottlenecks, among other related matters. The Offerings are not intended for, or to meet, any sustainability, carbon, or cyber regulatory compliance requirements. You agree and acknowledge that Honeywell is not responsible or liable for any damage, claims or injury arising out of or in any way related to your access or use of, or action, inaction, or reliance on information contained within or transmitted by the Offering, and you expressly accept this limitation when subscribing to the Offering. You agree that you will not rely on the Offering for any life safety, critical or other regulatory compliance purposes. The Offering is not a substitute for a third-party monitored emergency notification system. We make no representation or warranty that your use of the Offering will improve your operations, safety, sustainability, cyber capabilities, or reliability. **C**. The Offering(s) may require Firewall rule configurations made on the Customer 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 Offering(s) may allow you to enter your own analytics or set points, dashboard and/or configurations. We do not guarantee the reliability or accuracy of the Offering's output, and you are solely responsible for its use and interpretation. Any default analytics and set points provided in the Offering are intended to help inform your decisions, but ultimately, you are responsible for ensuring that all notifications and alarms set in your instance, based on the default analytics, and set points, are accurate.

   Any analytics and set points provided by you are at your discretion and we are not responsible for the recommendations provided by the Offering(s) or your actions taken because of these analytics and set points. Any analytics and set points provided in the Offering are intended solely to help with your decisions but ultimately you are responsible and liable for ensuring that all notifications and alarms set in your instance are handled appropriately for your business. Actions taken on alarms (including closing, deleting, or snoozing) are visible to all authorized users and applicable across the entire Site. The Offering is not designed or intended for real-time or time-critical control of your 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. You will not upload, or permit the uploading of, sensitive personal data into the Offerings (including but not limited to social security numbers, bank account numbers, credit card numbers, geolocations) and industry specific sensitive or regulated data. You are solely responsible to confirm that your use of the Offering(s) is in conformance with any applicable third-party requirements, including service and/or warranty requirements. We may provide self-service training modules to assist with the provision of Offering training to your Users. On-site training may be available at an additional fee.

D. Customer Site Readiness

In order to deploy, implement and maintain the SaaS Offerings at each Site, as conditions precedent, Customer understands and agrees to ensure that each Site meets minimum Site readiness requirements as provided by Honeywell and as required per the applicable Offering ("**Site Readiness**"). Honeywell is not liable for any delays or impairment of Offering functionality caused by Customer's failure to provide and maintain Site Readiness, and Customer will remain responsible for all payments and obligations provided in an Order Form irrespective of any such delays or failures. For Site Readiness areas identified below as "Pre-Site Connection", these readiness conditions must be met by Customer before any Honeywell Implementation work can commence on the SaaS Offering deliverables in this Order Form. Other areas not identified as Pre-Site Connection must be maintained by Customer as ongoing Site Readiness responsibilities during the Term. The minimum Site Readiness requirements that Customer 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 - Customer IT team access and IT technical information to connect Offerings;
- Pre-Site Connection - Approved firewall to deny inbound and restrict outbound access to Customer systems;
- Pre-Site Connection - Connectivity to the internet with suitable reliability and bandwidth to uplift the projected data rates;
- Dedicated Customer 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 Offerings;
- 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:** Asset Reliability includes SaaS and the Hardware price in the Order Form, which may include cellular and/or Wi-Fi enabled sensors and sensor accessories, such as sensor mounts. Hardware is sold to you upon your purchase and full payment in advance. . Following your full payment and delivery of the Hardware you purchase, title to, and ownership of, the Hardware will transfer to you. Except as aforesaid or as expressly permitted under the Agreement, you do not have any ownership right, title or interest in or to the Hardware. You agree to only use the Hardware in accordance with the written instructions, operating parameters, and specifications ('Hardware Documentation') made available by us. You acknowledge that failure to follow the Hardware Documentation may result in damage to the Hardware (for which you are liable) and/or adversely impact the performance of this feature, which may void your equipment warranty. You assume risk of loss or damage for the Hardware following delivery to the Site location specified in the Order Form.

2. **Hardware Installation and Maintenance:** The Hardware is designed for non-invasive installation. You are required to install and secure the Hardware, unless otherwise indicated in the Order Form. If you install the Hardware, you will abide by all instructions and Hardware Documentation, including for installation and configuration, and are solely responsible for any installation issues. For Hardware sensors to adhere to your systems, you understand that installation may require magnet, epoxy resin, or adherence to studs, as applicable to your Site. You 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. You must ensure that the Hardware remains as installed during your subscription and you maintain Site protections in place to prevent tampering or interference. You are solely responsible for any costs, expenses, damages and/or repairs relating to the installation, tampering and/or removal of the Hardware.

3. **Connectivity:** The Hardware sensors provided as part of the Asset Reliability may come pre-installed with their own sim card which must only be used in conjunction with that specific sensor. You are not permitted to remove sim cards from sensors. Unless specified otherwise in the Order Form, you must use the cellular data connectivity service provided with the cellular sensors and you are not permitted to procure your own cellular service. To ensure satisfactory performance of Asset Reliability you may be required to provide information about your 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 your responsibility to ensure that the Site of the Hardware installation has sufficient cellular or Wi-Fi coverage to enable Asset Reliability to function properly. You acknowledge 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. We are not responsible for connectivity issues, and we give no warranty or guarantee as to network coverage, quality or availability. We are also not responsible for lost data and you agree to implement adequate backup storage.

4. **Cellular Data Usage:** For cellular enabled sensors, Asset Reliability includes data connectivity services, and the SaaS Subscription Fee includes cellular data of 30MB per month per sensor. We reserve the right to charge additional fees if the cellular data usage exceeds 30MB. We recommend that you 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
>1600	Max 6

5. **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, poor connectivity, operation outside specified environmental conditions or otherwise failing to follow the Hardware Documentation may reduce the expected battery life. You are responsible for any battery replacement required. We will repair or replace, in our discretion, defective Hardware provided as part of Asset Reliability unless failure is caused by tampering, abuse, damage, or negligence caused by you, including by your installation, or other unauthorized modification.

6. **Third Party Service Providers**: We may use third party service providers in the provision of Asset Reliability and in such case, you acknowledge that Input Data may be processed or used by such third-party service providers.

7. **Termination:** Upon termination or expiry of your subscription to Asset Reliability, your access to and use of the Asset Reliability solution will be discontinued.