Honeywell Remote Building Manager Offering Descriptions and Terms

Version: 1.0

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

Offerings	Description
Honeywell Remote Building Manager	Honeywell Remote Building Manager (RBM) is a cloud-based supervisor that provides access to building management systems (BMS) that enables Users to monitor and control a single site or a portfolio of multiple sites. RBM is a system agnostic solution compatible with Niagara-based systems, Enterprise Buildings Integrator (EBI), and third-party systems with following BACnet over IP and Modbus protocols. RBM enables remote triaging and issue resolution, remote connection to linked gateways to perform diagnostics, lifecycle and obsolescence tracking of connected equipment and assets with intuitive configurable dashboards to track certain Key Performance Indicators (KPI) of buildings. RBM provides self-service on-boarding and commission processing through its Onboarding Portal. Once the site commissioning is done, the standardized supervisor dashboard pages get populated automatically along with the portfolio dashboard bringing consistency while managing a multi-site portfolio. The RBM features available are set forth below. The specific features for User will be set forth in the Order. • Remote Building Manager Supervisor • Opportunity Assessment • Life cycle management • Unified Portal – KPI Dashboard

B. Offering Package and Feature Descriptions

Product Features	Description
Self Service Onboarding Portal	System integrators/ channel partners have access to a self-service onboarding portal to onboard new sites, manage users and subscription.
Remote Building Manager Supervisor	RBM supervisor consists of the following features: • **Asset Modelling:** This feature allows user configuration through the cloud, like creating new equipment, renaming equipment, and assigning point roles to the point. Changes made in the cloud are synced with the gateway. • **Basic portfolio dashboard** provides: ○ **Map view**: overall indication of the portfolio site

	○ **Alarm**: Categorized with High Medium and Low severity with easy configuration. ○ **Schedules & Overrides:** This widget displays all necessary information at a glance. • **Site Summary Dashboard** provides an overview of the site status connectivity, schedule & override widget, alarm widget, active high alarm widget, and point list view with a summary tab. • **Equipment / Device dashboard** displays the equipment details and allows users to update settings. The details of points displayed depend on the equipment type, like AHU, VAV, FCU, etc. It displays information such as equipment information & connectivity widget, equipment summary widget (AHU, VAV & FCU equipment), active alarm widget, trend dashboard, point list view, and schedule. • **Point List View** allows sorting points lists by name, equipment / device name, value, area and it also allows users to apply quick filters, viewpoint details, point to trend mapping, point write / set action, multi / batch point write, point override and clear override, as well as advanced filters. This feature is designed to support a maximum of 75,000 data points. If your data exceeds 75,000 data, your performance may be affected, and the feature might not work as expected. • **Schedule Management** allows viewing connected controller weekly schedules in the supervisor dashboard (single schedule / equipment or device) and editing the schedule from the supervisor as well as syncing to the gateway. • **Alarm management** allows viewing BACnet controller and gateway-based alarms, trends associated with a point, activity log, and alarm acknowledgment. • **User Settings** allows users to set the language, unit, date and time, theme customization, and modify email alarm notifications.
Opportunity Assessment	Opportunity Assessment enables the identification of maintenance needs and energy-saving opportunities through data-informed operational enhancements. Key features include: • **Telemetry-Driven Analysis**: Utilizes near real-time and historical building telemetry data, structured through ontology-based models, to assess system performance and operational behavior. • **Standards-Based Benchmarking**: Evaluates building performance against recognized industry benchmarks to identify inefficiencies and areas of underperformance. • **Quantification of Financial Impact**: Provides data-driven estimates of potential cost savings associated with identified improvements, supporting strategic investment and budgeting decisions.
Asset Life Cycle Assessment	Asset Life Cycle Assessment provides near real-time visibility into the status and lifecycle of building assets, enabling proactive management and strategic planning. Core capabilities include: • **Real-Time Asset Monitoring:** Delivers continuous status updates on building assets using data-driven insights to support operational awareness. • **Lifecycle Risk Assessment:** Displays current lifecycle stages of assets, highlighting associated risks and offering actionable recommendations for mitigation. • **Modernization Guidance:** Identifies outdated or obsolete assets and provides tailored upgrade or replacement recommendations to maintain operational efficiency. • **Obsolescence Reporting Tools:** Enables generation and export of detailed asset obsolescence reports in both PDF and Excel formats for documentation and analysis. • **Customer Engagement Support:** Facilitates proactive asset planning and budgeting discussions with stakeholders, enhancing transparency and collaboration. • **Revenue Optimization Insights:** Uncovers opportunities to replace obsolete equipment, potentially unlocking new revenue streams and improving service delivery.
Unified Portal – KPI Dashboard	Unified Portal – KPI Dashboard supports the optimization of managed building operations by delivering clear, actionable insights into energy consumption, occupant comfort, asset health,

	and overall system performance. Key features include: • **Unified Application Platform**: Integrates multiple operational tools and applications into a single, cohesive interface to streamline user experience and reduce system complexity. • **Centralized Remote Operations**: Facilitates enhanced collaboration and coordination across teams through a shared, cloud-based information environment. • **Configurable Data Dashboards**: Offers customizable dashboards that allow users to visualize and track key performance indicators and operational metrics relevant to their specific sites. • **Near Real-Time Monitoring**: Provides access to near real-time data from connected systems, enabling proactive performance management and timely decision-making. •

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