CONDITION-BASED MAINTENANCE +

1. **GENERAL**

1.1 **<u>Service Definition</u>.** Condition-Based Maintenance (the CBM Service) allows Customer and its Users to remotely monitor, access, and manage industrial equipment via sensor data. The CBM Service consists of: (1) the CBM Agent for Communication Devices; and (2) the CBM Platform, for gathering diagnostics, KPIs and other sensor data from Internet of Things (IoT) endpoints via the CBM Agent, and creating workflows, alerting and analytics based on that sensor data; and (3) configuration and setup services (Setup Service) for the CBM Platform.

1.1.1 **Platforms.** Except where explicitly stated otherwise, these terms apply to Optimized Service (denoted with a "+" and sometimes referred to as Rapid Delivery) and Non-Optimized Service.

1.2 <u>Standard Features</u>

1.2.1 **Basic Availability.** The CBM Service provides a setup and operation of hosted platform-as-a-service for remote monitoring and management of industrial assets.

1.2.2 **Use Restriction.** The CBM Service is provided hereunder for Customer's use and may not be resold or otherwise provided to third parties, either directly or indirectly, except as expressly permitted herein. Customer may provide access to its Customers to the CBM Platform when offered as part of a Customer solution that incorporates the CBM Service for remote management of IoT equipment sold, leased or otherwise distributed by Customer.

1.3 <u>License</u>

1.3.1 **Limited License.** Verizon grants Customer a limited, revocable, non-assignable, non-exclusive license during the Service Term, to access and use the CBM Service as permitted herein. Customer will use the CBM Service only for lawful purposes. Customer will not reverse engineer, decompile, create derivative works, or in any way infringe or misappropriate the intellectual property rights embodied in the CBM Service.

1.3.2 **Reservation of Rights.** All other rights in and to the CBM Service are hereby reserved by Verizon Wireless and its licensors, including but not limited to all of the intellectual property rights embodied within the CBM Service

1.4 **Customer Responsibilities**

1.4.1 **Communication Devices.** Customer has full responsibility for acquiring, installing, operating and maintaining all Communication Devices.

1.4.2 **Connectivity.** CBM does not include any connectivity service, whether cellular, wi-fi or some other communication technology. Customer is responsible for purchasing, configuring and maintaining connectivity as required for using CBM, including, if and where applicable, wireless connectivity for Communication Devices.

1.4.3 **Account Activity.** Verizon will provide Customer with account credentials to access the CBM Platform and administer User accounts. Customer shall permit access to the CBM Platform only to Users. Users may include customers of Customer who may be provided limited access to the CBM Platform as permitted by Section 1.2.2 (Use Restriction). Customer shall be responsible for all activity under its account for the CBM Platform, including without limitation the acts and omissions of its Users. Customer agrees to immediately notify Verizon Wireless of any unauthorized access to the CBM Platform, account, or any other breach of security upon becoming aware of such unauthorized access.

1.5 **Customer Data**

1.5.1 **Use of Customer Data.** By using the CBM Service, Customer consents to Verizon's collection and use of Customer Data in accordance with the terms of the Verizon Privacy Policy, located at https://www.verizon.com/about/privacy/. Customer is responsible for ensuring that it has obtained all necessary rights and approvals to permit Verizon, its affiliates and contractors, to access and use Customer Data as described in the Privacy Policy, including express consent where required by applicable laws.

1.5.2 **User Personal Information.** If Customer collects and/or shares personal information from Users in connection with the CBM Service, Customer must (1) disclose to such Users details regarding its collection, use, treatment, storage and disposal of any such information, and (2) obtain consent from Users before collecting and sharing their personal information.

2. SETUP SERVICE

2.1 **Scope**

2.1.1 **Description.** Verizon will perform certain work in order to set up Customer's CBM Service deployment and configure the CBM Platform for Customer's requirements.

2.1.2 **Activities.** Setup Service can include some (but not necessarily all) of the following activities, based on requirements agreed upon between Verizon and Customer.

- Connection of Communication Devices to the CBM Platform, including selection of parameters required for monitoring health, performance and reliability of connected assets.
- Deployment of CBM Agent to Communication Devices.
- Set up of secure user access and environment with authentication and editable user permissions.
- Application configuration in the CBM Platform, which may include:
  - o Customer branded web application.
  - o Sub accounts (organization of end customer data).
  - o Asset summary – equipment by customer by location.
  - o Map based view of equipment.
  - o Monitor and log key data points as set forth in a requirements definition.

  - Maintenance module – usage based notification of service intervals using one of the above data points.
  - Alerts /alarms – advisory/fault records. display current alarms/events and save up to 100 past events.
  - Email notification on alerts/faults/ maintenance module
  - Custom widgets.
- Testing to verify proper data transfer.

3. ADDITIONAL TERMS

3.1 WARRANTIES AND DISCLAIMERS.

3.1.1 **Limited Warranty.** Verizon warrants that (i) it has the authority and right to provide the CBM Service to Customer, including the right to grant license(s) as set forth herein; and (ii) all work performed hereunder will be performed in professional and workmanlike manner in accordance with relevant industry standards.

3.1.2 **DISCLAIMER.** EXCEPT AS EXPRESSLY PROVIDED HEREIN, VERIZON PROVIDES THE CBM SERVICE “AS IS” AND “AS AVAILABLE” AND DISCLAIMS ALL REPRESENTATIONS OR WARRANTIES TO THE FULLEST EXTENT PERMITTED BY LAW, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THAT THE CBM SERVICE SHALL BE ERROR-FREE OR COMPLETELY SECURE.

3.1.3 **LIMITATION OF LIABILITY.** VERIZON DISCLAIMS ANY AND ALL LIABILITY RELATED TO ANY OUTAGE, DOWNTIME, INTERRUPTION, BREAKDOWN OR UNAVAILABILITY (FOR MAINTENANCE, UPGRADES, UPDATES OR OTHERWISE) OF THE CBM PLATFORM. NEITHER PARTY SHALL BE LIABLE FOR LOST DATA, LOST PROFITS, LOST REVENUES, BUSINESS INTERRUPTION, OR ANY OTHER INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES. OTHER THAN FOR INDEMNIFICATION OR PAYMENT OBLIGATIONS, EACH PARTY’S AGGREGATE LIABILITY FOR CLAIMS AND DAMAGES IN CONNECTION WITH THE AGREEMENT IS LIMITED TO THE LESSER OF (i) DIRECT DAMAGES PROVEN BY THE OTHER PARTY, OR (ii) THE AMOUNT OF FEES OR CHARGES PAID FOR THE CBM SERVICE DURING THE 12-MONTH PERIOD BEFORE THE DATE ON WHICH ANY CLAIM AROSE.

3.1.4 **Indemnification.** Customer agrees to defend, indemnify, and hold harmless Verizon and its employees, officers, directors, agents, vendors, subcontractors, parents and affiliates from and against any losses, liabilities, damages, penalties, fines, claims, causes of action, and demands brought by any User or third party (including costs, expenses, and reasonable attorneys’ fees and allocable cost of in-house counsel) resulting from or arising out or relating to: (a) Customer’s breach of these terms, or (b) non-compliance with applicable laws.

3.2 Device Best Practices

3.2.1 **Device Best Practices.** In using Communication Devices with the CBM Service, Customer agrees to comply with the following best practices:

- Change default passwords for router administration credentials. Password should follow a corporate standard that defines minimum number of character, type and number of characters required, and timeframe for expiration.
- Refrain from using the same password on more than one device. Passwords must be unique.

- Log out of admin interface when finished with tasks. Do not leave open the admin interface when not in use.
- Disable remote management on the router if not needed. If remote admin is needed, restrict access to only known IP addresses.
- For administration of the router, use SSL or SSH whenever possible instead of plain unencrypted access.
- Monitor for suspicious activity using device logging and status information.
- Keep firmware up to date to ensure security fixes/ patches are recent.
- Isolate LAN or any other network that do not need to communicate together.
- Limit administrative access to the device to only those who require it. Build alternative user accounts with limited capabilities for others that need access to the device but not admin level rights.
- Disable any protocols or features that are not in use.
- Disable or restrict settings such as DHCP, ping, trace route, telnet, etc. to reduce visibility to attacks.
- Develop and comply with an acceptable usage policy for staff that describes what is permitted on the network and what best practices staff should follow.
- Place devices in locations that provide physical security. Devices should not be in open areas where un-authorized individuals can gain physical access.
- Wired ports not in use should be disabled.
- Ports in use should use 802.1x or MAC authentication to prevent unauthorized devices to connect to the network.
- Select the most secure features when possible (e.g., use AES instead of DES).
- Real time clock on devices should be configured accurately. Connect devices to reliable NTP source.
- Disable any file sharing, NAS or USB ports/options.
- Maintain backups of device configurations.
- If wireless capabilities on devices are not used, disable feature.
- Change default SSID to a name the does not easily identify the device, company, brand, or location of the device.
- Use the strongest wireless encryption supported by device. Avoid using no encryption or WEP.
- Disable wireless access except when functionality is required.
- Disable WPS if supported on device.

4. **DEFINITIONS.** The following definitions apply to IoT Connectivity, in addition to those identified in the Master Terms.

Term	Definition
CBM Agent	A device application that enables a Communication Device to transmit sensor data to the CBM Platform.
CBM Platform	A hosted platform for ingesting, analyzing and displaying IoT sensor data and automating workflows for remote management of industrial equipment.
CBM Service	Condition-Based Maintenance. An industrial IoT solution for remote monitoring and management of industrial equipment based on IoT sensor data.
Communication Device	A device capable of running the CBM Agent to transmit IoT sensor data to the CBM platform.
Service Term	The duration of the term of the CBM Service.
User	An employee, contractor or agent of Customer or Customer's customers who has access to the CBM Platform.