

Terms of Use for HCL OneDB

This Terms of Use for HCL OneDB (“Terms of Use”), the Master License Agreement (available at: <https://www.hcltechsw.com/wps/portal/resources/master-agreements>), the Order, and the AWS Customer Agreement (available at: <https://aws.amazon.com/agreement/>) together make the complete agreement (“Agreement”) for the acquisition of the HCL OneDB solution.

Any capitalized terms used but not defined in this Terms of Use shall have the meanings given to such terms in the other documents of the Agreement.

In the event of a conflict regarding the subject matter herein, this Terms of Use prevail. By ordering, accessing, or using the HCL OneDB solution, Customer agrees to this Terms of Use.

1. HCL OneDB is sold via the AWS Marketplace.
2. Charge Metrics. HCL OneDB is sold under the charge metric(s) as specified in the Order.
3. Charges and Billing. The amount payable for HCL OneDB is specified in an Order.
 - a. Set-Up Charges - Set-Up Services are purchased on a per engagement basis and will be billed at the rate specified in the Order.
 - b. Partial Month Charges - A partial month charge as specified in the Order may be assessed on a pro-rated basis.
4. Technical Support. Technical support (“Support”) for HCL OneDB is provided via online forums and an online problem reporting system. Support is offered with HCL OneDB and is not available as a separate offering. Upon purchase of the HCL OneDB solution, Customer is automatically enrolled in standard Support for the duration of service subscription set forth in the Order and HCL shall provide Support in accordance with the then current Support Guide posted at <https://support.hcltechsw.com/csm>. While Support is in effect, HCL may make available defect corrections, restrictions, bypasses, new versions, releases, or updates available as part of Support. Any items provided under Support are subject to the same terms, conditions, usage limitations and restrictions as the HCL One DB solution. Notwithstanding the foregoing, the following Severity levels apply to HCL OneDB:

Severity 1

Severity Definition - Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.

Response Time Objectives - Within 1 hour

Response Time Coverage - 24x7

Severity 2

Severity Definition - Significant business impact: A service business feature or function of the service is severely restricted in its use or Customer is in jeopardy of missing business deadlines.

Response Time Objectives - Within 2 business hours

Response Time Coverage - M-F business hours

Severity 3

Severity Definition - Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations.

Response Time Objectives - Within 4 business hours

Response Time Coverage - M-F business hours

Severity 4

Severity Definition - Minimal business impact: An inquiry or non-technical request.

Response Time Objectives - Within 1 business day

Response Time Coverage - M-F business hours

5. Additional Terms.

- a. General. Customer agrees that HCL may publicly refer to Customer as a subscriber to the HCL OneDB solution in a press or marketing communication.
- b. Personal Information and Regulated Data. The HCL OneDB solution is not designed to meet or adhere to any specific security requirements for regulated content, such as personal information or sensitive personal information. Customer is responsible to determine if the HCL OneDB solution meets Customer's needs with respect to the type of content Customer uses in connection with the HCL OneDB solution.
- c. Security. Customer acknowledges that the OneDB solution is controlled by Customer and Customer agrees to maintain the HCL OneDB solution in accordance with Customer's security standards and those required under the AWS Customer Agreement. Further, HCL will not be responsible for any claims, losses, and liabilities or damages relating to any claims (including loss of data) made against HCL as a result of Customer's failure to maintain security standards for the HCL OneDB solution.
- d. Encryption. HCL OneDB native encryption is included for all configurations of the HCL OneDB solution. HCL OneDB native encryption encrypts Customer's HCL OneDB database and provides secure local key management based on Public Key Cryptography Standard #12 (PKCS#12). HCL provides Customer with an initial HCL OneDB server with encryption at rest. Customer is responsible for any change, and further configuration, implementation, and maintenance of encrypted HCL OneDB databases using the included HCL OneDB options, utilities, and documentation.
- e. Derived Benefit Locations. Where applicable, taxes are based upon the location(s) Customer identifies as receiving benefit of the HCL OneDB solution. HCL will apply taxes based upon the business address listed when ordering HCL OneDB as the primary benefit location unless Customer provides additional information to HCL. Customer is responsible for keeping such information current and providing any changes to HCL.
- f. Customer Obligations. Customer is obligated to install patches for HCL OneDB, the operating system, and other software in a timely manner to avoid defects, avoid security issues, and maintain currency with new functionality.
Customer may:

- Only install and run software on the HCL OneDB solution that is directly related to performing or supporting use of data through the pre-installed HCL OneDB software. Customer is prohibited from installing or using any other software of any kind on the HCL OneDB solution.
- Install additional open source packages for use with HCL OneDB on the nodes. HCL is not obligated to support these packages and is not responsible for impacts to the performance of HCL OneDB (i.e. HCL OneDB, the operating system, or the hardware platform as a whole) due to these additional packages.

Customer may not:

- Resell direct access to a service or cloud service to a third party.