ORACLE

Oracle Cloud Hosting and Delivery Policies

Effective Date: February 2024; Version 3.6

TABLE OF CONTENTS

OVERVIEW

These *Oracle Cloud Hosting and Delivery Policies* (these "Delivery Policies") describe the Oracle Cloud Services ordered by You. These Delivery Policies may reference other Oracle Cloud policy documents; any reference to "Customer" in these Delivery Policies or in such other policy documents shall be deemed to refer to "You" as defined in Your order. All commitments in these Delivery Policies apply to production Cloud Services unless otherwise specified.

References in these Delivery Policies to a Cloud Services' "Data Center Region" refers to the geographic region listed in Your order for such Services or, if applicable, the geographic region that You have selected when activating the instance of such Services. For purposes of the Data Center Region applicable to Your ordered Cloud Services, the following applies:

- "Europe" refers to the member countries of the European Union, the United Kingdom, and Switzerland, collectively; and
- "APAC" refers to the Asia-Pacific geography, except China as Oracle has no data centers in China
- "North America" refers to geographical regions made up of the continental United States of America and Canada; except where the entity purchasing Cloud Services elects to be initially provisioned in the country of Mexico, in which case, North America refers to the geographical regions made up of the continental United States of America, Canada and Mexico.

With respect to Your ordered Oracle Cloud Services, Your Content will be stored in the Data Center Region applicable to such Services. Oracle may replicate Your Content to other locations within the identified Data Center Region in support of data redundancy. Capitalized terms that are not otherwise defined in these Delivery Policies shall have the meaning ascribed to them in the Oracle agreement, Your order or the policy, as applicable. These Delivery Policies are updated on a biannual basis.

Your order or Oracle's Service Specifications (as defined in Your agreement for Oracle Cloud Services which includes Oracle Cloud Services Pillar documentation, Service Descriptions and additional definitions provided in the Oracle Cloud Services Agreement) may include additional details or exceptions related to specific Oracle Cloud Services. The Oracle Cloud Service Pillar documentation, the Service Descriptions and the Program Documentation for Oracle Cloud Services are available at www.oracle.com/contracts.

Oracle Cloud Services are provided under the terms of the Oracle agreement, Your order, and Service Specifications applicable to such Services. Oracle's delivery of the Oracle Cloud Services is conditioned on Your and Your Users' compliance with Your obligations and responsibilities defined in such documents and incorporated policies. These Delivery Policies, and the documents referenced herein, are subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of performance, functionality, security, or availability of the Oracle Cloud Services provided during the Services Period of Your order.

Oracle Cloud Services are deployed at data centers or third-party infrastructure service providers retained by Oracle, with the exception of Oracle Cloud at Customer Services. Oracle Cloud at Customer Services are Public Cloud Services that are deployed at Your data center or at a third-party data center retained by You. You may purchase these Services standalone or they may be deployed as the underlying platform for other Oracle Cloud Services. For Oracle Cloud at Customer Services, Oracle will deliver to Your data center certain hardware components, including gateway equipment, needed by Oracle to operate these Services. You are responsible for providing adequate space, power, and cooling to deploy the Oracle hardware (including gateway equipment) and for ensuring adequate network connectivity for Oracle Cloud Operations to access the services. Oracle is solely responsible for maintenance of the Oracle hardware components (including gateway equipment).

These Delivery Policies do not apply to Oracle BigMachines Express or such other Oracle Cloud offerings as specified by Oracle in Your order or the applicable Service Descriptions.

1. ORACLE CLOUD SECURITY POLICY

1.1 Oracle Information Security Practices - General

Oracle has adopted security controls and practices for the Oracle Cloud Services that are designed to protect the confidentiality, integrity, and availability of Your Content that is hosted by Oracle in Your Oracle Cloud Services and to protect Your Content from any unauthorized processing activities such as loss or unlawful destruction of data. Oracle continually works to strengthen and improve those security controls and practices.

Oracle Cloud Services operate under practices which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected. Oracle Cloud Services are aligned with National Institute of Standards and Technology ("NIST") 800-53 and 800-171.

Oracle Cloud information security practices establish and govern areas of security applicable to Oracle Cloud Services and to Your use of those Oracle Cloud Services.

Oracle personnel (including employees, contractors, and temporary employees) are subject to the Oracle information security practices and any additional policies that govern their employment or the services they provide to Oracle.

Oracle takes a holistic approach to information security, implementing a multi-layered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance and oversight.

For those Oracle Cloud Services which enable You to configure Your security posture, unless otherwise specified, You are responsible for configuring, operating, maintaining, and securing the operating systems and other associated software of these select Oracle Cloud Services (including Your Content) that is not provided by Oracle. You are responsible for maintaining appropriate security, protection, and backup of Your Content, which may include the use of encryption

technology to protect Your Content from unauthorized access and the routine archiving of Your Content.

1.2 Physical Security Safeguards

Oracle employs measures designed to prevent unauthorized persons from gaining access to computing facilities in which Your Content is hosted such as the use of security personnel, secured buildings, and designated data center premises. Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Oracle controlled co-locations/data centers currently include, for example:

- Physical access requires authorization and is monitored
- All employees and visitors must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed while onsite
- Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards

Additional physical security safeguards are in place for Oracle-controlled Cloud data centers, which currently include safeguards such as:

- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles
- Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management
- Safeguards related to environmental hazards
- Any physical movement of equipment is controlled by hand-delivered receipts and other authorized change control procedures
- Network cables are protected by conduits and, where possible, avoid routes through public areas

This section does not apply to Oracle Cloud at Customer Services. You must provide Your own secure computing facilities for the hosting and operation of the Oracle Cloud at Customer Services-related hardware (including the gateway equipment) and network connections required for Oracle to provide the Oracle Cloud at Customer Services.

1.3 System Access Controls

Oracle policies require the following controls to be applied: authentication via passwords and/or multi-factor authentication, documented authorization controls, and logging of access. All remote access to the Oracle Cloud Network by Oracle personnel that have access to Your Content is restricted through the use of a Virtual Private Network which utilizes multi-factor authentication. In addition to the required use of a Virtual Private Network, before Oracle personnel are granted access to the Oracle Cloud Network, Oracle performs device posture checks and has in place controls, such as

bastion hosts. Oracle prohibits (through both policy and technical controls) the use of personal devices to access the Oracle Cloud Network and the Oracle Cloud Services.

For Cloud Services hosted by Oracle: (i) log-ins to Cloud Services are logged and (ii) logical access to the data centers is restricted and protected.

1.4 Data Access Controls

For service components managed by Oracle, Oracle's access to Your Content is restricted to authorized staff.

With respect to Oracle personnel accessing the Oracle Cloud Services (including Your Content residing in the Oracle Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties." In addition, Oracle provides a mechanism by which You control Your Users' access to the Oracle Cloud Services and to Your Content.

1.5 User Encryption for External Connections

Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128 bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each release of Oracle Cloud Services will be made available via a portal accessible to You or in the corresponding Service Description for the Oracle Cloud Services. In some cases, a third party site that You wish to integrate with the Oracle Cloud Services, such as a social media service, may not accept an encrypted connection. For Oracle Cloud Services where HTTP connections with the third party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.6 Input Control

The source of Your Content is under Your control and Your responsibility, and integrating Your Content into the Oracle Cloud Services, is managed by You.

1.7 Data and Network Segregation

Your Content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud Services. All Oracle Cloud networks are segregated from Oracle's corporate networks.

1.8 Confidentiality and Training

Oracle personnel are subject to confidentiality agreements and are required to complete information-protection awareness training upon hiring. Thereafter, all Oracle personnel must complete training periodically in accordance with applicable Oracle security and privacy awareness training policies.

1.9 Asset Management

Oracle is responsible for the protection and inventory of Oracle's Cloud Services assets. The responsibilities may include reviewing and authorizing access requests to those who have a business need and maintaining an inventory of assets.

You are responsible for the assets You control that utilize or integrate with the Oracle Cloud Services, including determining the appropriate information classification for Your Content, and whether the documented controls provided by Oracle Cloud Services are appropriate for Your Content. You must have or obtain any required consents or other legal basis related to the collection and use of information provided by data subjects, including any such consents or other legal basis necessary to provide the Oracle Cloud Services.

1.10 Oracle Internal Information Security Policies

Oracle Cloud information security policies establish and govern areas of security applicable to Oracle Cloud Services and to Your use of Oracle Cloud Services. Oracle personnel are subject to the Oracle Corporate Information Security Policies and any additional policies that govern their employment or the services they provide to Oracle. Oracle's Information Security Program ("ISP") is comprised of documented policies that consider risk factors including cyber and security factors, with accompanying derivative procedures, standards and guidelines required for the effective operationalization of policy. Oracle's ISP is designed to ensure the confidentiality, integrity, privacy, continuity and availability of Your Content that is hosted by Oracle in Your Oracle Cloud Services through effective security management practices and controls. Oracle's ISP is reviewed annually by the Oracle Security Oversight Committee and updated as required.

1.11 Internal Security Reviews and Enforcement

Oracle employs internal processes for regularly testing, assessing, evaluating and maintaining the effectiveness of the technical and organizational security measures described in this section.

1.12 External Reviews

Oracle may conduct independent reviews of Oracle Cloud Services utilizing third parties in the following areas (the scope of any such reviews may vary by Service and country):

- SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports (based upon Trust Services Criteria)
- Other independent third-party security testing to review the effectiveness of administrative and technical controls

Relevant information from these reviews may be made available to customers.

1.13 Oracle Software Security Assurance

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by

customers, or delivered through Oracle Cloud. The OSSA program is described at https://www.oracle.com/corporate/security-practices/assurance/.

1.14 Security Logs

Logs are generated for security-relevant activities on operating systems. Systems are configured to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors. Oracle reviews logs for forensic purposes and incidents; identified anomalous activities feed into the incident management process. Security logs are stored within the Security Information and Event Management system (or equivalent system) in a native, unaltered format and retained in accordance with Oracle's internal policies. Such logs are retained online for a minimum of 1 year. These logs are retained and used by Oracle for our internal security operations of the Oracle Cloud Services.

1.15 Other Customer Security Related Obligations

You are responsible for:

- Implementing Your own comprehensive system of security and operational policies, standards and procedures, according to Your risk-based assessments and business requirements
- Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to the Oracle Cloud Services
- Managing client device security controls, so that antivirus and malware checks are performed on data or files before importing or uploading data into the Oracle Cloud Services
- Maintaining Customer-managed accounts according to Your policies and security best practices
- Additionally, for Oracle Cloud at Customer Services, You are responsible for the following:
    - Adequate physical and network security
    - Security monitoring to reduce the risk of real time threats and prevent unauthorized access to Your Oracle Cloud Services from Your networks; this includes intrusion detection systems, access controls, firewalls and any other network monitoring, and any management tools managed by You.

2. ORACLE CLOUD SERVICE CONTINUITY POLICY

2.1 Oracle Cloud Services High Availability Strategy

Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the Services. Data centers retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and/or storage.

2.2 Oracle Cloud Services Backup Strategy

Oracle periodically makes backups of Your Content in your instance of the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services and may also be stored at an alternate location for retention purposes. A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. Oracle typically does not update, insert, delete or restore Your data on Your behalf. However, on an exception basis and subject to written approval, Oracle may assist You to restore data which You may have lost as a result of Your own actions.

For Oracle Cloud Services which enable You to configure backups in accordance with Your own policies, You are responsible for performing backups and restores of Your Content. Additionally, You are encouraged to develop a business continuity plan to ensure continuity of Your own operations in the event of a disaster.

2.3 Oracle Business Continuity

Oracle will at all times during the term maintain a plan as it pertains to Oracle's internal operations with the goal of minimizing any disruption to the provision of services if any disaster, disruption or force majeure event occurs ("BC Plan").

The BC Plan establishes, documents and implements processes, procedures and controls to ensure the security provisions applicable to the Oracle Cloud Services are not diminished in the event the BC Plan is invoked. The purpose of the BC Plan is to provide, among other things, resilience for Oracle's internal operations for the continuity and maintenance of the Oracle Cloud Services regardless of cause.

3. ORACLE CLOUD SERVICE LEVEL AGREEMENT

3.1 Hours of Operation

The Oracle Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth in the Oracle agreement, Your order and this *Oracle Cloud Service Level Agreement*.

3.2 Service Availability

Commencing at Oracle's activation of Your Oracle Cloud Service, Oracle works to meet the Target Service Availability Level, or Target Service Uptime of 99.9%. This is in accordance with the terms set forth in the Oracle Cloud Service Pillar documentation for the applicable Oracle Cloud Service (or such other Target Service Availability Level or Target Service Uptime specified by Oracle for the applicable Oracle Cloud Service in such documentation).

The foregoing is contingent on Your adherence to Oracle's recommended minimum technical configuration requirements for accessing and using the Oracle Cloud Services from Your network infrastructure and Your user workstations as set forth in the Program Documentation for the applicable Oracle Cloud Services.

3.2.1 Measurement of Availability

Following the end of each calendar month of the applicable Services Period, Oracle measures the Service Availability Level or Service Uptime over the immediately preceding month by dividing the difference between the total number of minutes in the monthly measurement period and any Unplanned Downtime (as defined below) by the total number of minutes in the measurement period and multiplying the result by 100 to reach a percent figure.

$$\left(\frac{Number\ of\ minutes\ in\ the\ month - Number\ of\ minutes\ of\ unplanned\ downtime}{Number\ of\ minutes\ in\ the\ month}\right) * 100$$

Number of minutes in a 30 day month = 30 days * 24 hours in the day *60 minutes in an hour

Number of unplanned minutes in the month = minutes of unplanned downtime defined in the section "*Definition of Unplanned Downtime*".

Example: June has 30 days = 30*24*60 = 43,200 minutes in the month

If 90 minutes of unplanned downtime occurred in the month of June the equation would be:

$((43{,}200 - 90)/43{,}200) * 100$ = 99.8% Service Level Availability

3.2.2 Reporting of Availability

Oracle will provide you metrics on the Service Availability Level for Oracle Cloud Services that You purchased under Your order, either in a self-service manner or via a Service Request submitted by You to Oracle requesting the metrics.

3.2.3 Service Credits

You may receive Service Credits in the event that the Target Service Availability Level or Target Service Uptime for Oracle Cloud Services that You purchased under Your order is below the defined Target Service Availability Level or Target Service Uptime applicable to such Services. Service Credits are defined in the Oracle Cloud Service Pillar documentation or Service Descriptions applicable to Your purchased Oracle Cloud Services. Notwithstanding the provisions of this section, if Your order with Oracle or Service Specifications applicable to your order for a particular Oracle Cloud Service provides a right to receive a higher amount of Service Credits, then You may receive the Service Credits under the provision which provides for the highest amount of Service Credits to You, but You may not recover Service Credits under multiple provisions for the same event.

3.3 Definition of Unplanned Downtime

Oracle Cloud Services are deployed in resilient computing facilities with resilient infrastructure, redundant network connections, and power at each hosting facility.

"Unplanned Downtime" means any time during which a problem with the Oracle Cloud Services prevents Your connectivity. Unplanned Downtime does not include any time during which the Oracle Cloud Services or any Oracle Cloud Services component are not available due to: (i) scheduled maintenance, (ii) circumstances outside of Oracle's control and other force majeure events (e.g.,

outages initiated at Your request, outages caused by non-Oracle infrastructure such as electrical, network, telecommunication, or other connectivity equipment, security attacks, natural disasters, or political events), (iii) any actions or inactions of You, Your Users or any third party (other than any Oracle agents and contractors who Oracle has engaged to perform the applicable Oracle Cloud Services) or (iv) any suspension by Oracle permitted under Your Oracle agreement or Your order. In addition, with respect to Oracle Cloud at Customer Services, Unplanned Downtime also does not include downtime or other unavailability (i) of Your data center (e.g., due to maintenance) or (ii) occurring outside the on-site hours defined under Your order for Oracle Cloud Operations personnel at Your data center.

3.4 Monitoring

Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components. Oracle does not monitor, or address deviations experienced by any non-Oracle managed components used by You in the Oracle Cloud Services, such as non-Oracle applications.

3.4.1 Monitored Components

Oracle monitors the hardware that supports the Oracle Cloud Services, and generates alerts for monitored network components, such as CPU, memory, storage, database and other components. Oracle Cloud Operations staff monitors alerts associated with deviations to Oracle defined thresholds and follows standard operating procedures to investigate and resolve underlying issues.

3.4.2 Customer Monitoring & Testing Tools

Oracle permits You to conduct limited functional testing for Oracle Cloud Services in Your test instance. Specific rules for testing may be found in the Program Documentation.

Oracle regularly performs penetration and vulnerability testing and security assessments against Oracle Cloud infrastructure, platforms, and applications in order to validate and improve the overall security of Oracle Cloud Services. The Oracle Cloud Services Program Documentation outlines when and how You may assess or test any components that You manage or create in Oracle Cloud Services, including non-Oracle applications, non-Oracle databases, other applicable non-Oracle software, code, or the use of data scraping tools.

Oracle reserves the right to remove or disable access to any tools or technologies that violate the guidelines in this section or the applicable Oracle Cloud Services Program Documentation, without any liability to You.

4. ORACLE CLOUD CHANGE MANAGEMENT POLICY

4.1 Oracle Cloud Change Management and Maintenance

Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software that is provided by Oracle as part of the Oracle Cloud Services, to maintain operational stability, availability, security, performance, and currency of

the Oracle Cloud Services. Oracle follows formal change management procedures to review, test, and approve changes prior to application in the service.

Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer specific changes. Oracle Cloud Services change management procedures are designed to minimize service interruption during the implementation of changes.

Oracle reserves specific maintenance periods for changes that may require the Oracle Cloud Services to be unavailable during the maintenance period. Oracle works to ensure that change management procedures are conducted during scheduled maintenance windows (of which Oracle shall give advanced notice), while taking into consideration low traffic periods and geographical requirements.

Oracle will provide prior notice of modifications to the maintenance windows schedule. For Customer-specific changes and upgrades, where feasible, Oracle will coordinate the maintenance periods with You.

For changes that are expected to cause service interruption, the durations of the maintenance periods for scheduled maintenance are not included in the calculation of Unplanned Downtime minutes in the monthly measurement period for Service Availability Level (see the *Oracle Cloud Service Level Agreement* above). Oracle uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that cause service interruptions.

For Oracle Cloud Services which enable You to perform maintenance activities, You are responsible for configuring and maintaining the operating systems and other associated software.

4.1.1 Critical Security Maintenance

Oracle may be required to execute critical security maintenance in order to protect the security of the Oracle Cloud Services. Critical security maintenance is required to address an exigent situation (e.g., security vulnerability) with the Oracle Cloud Service or Oracle infrastructure that cannot be addressed except on an emergency basis. Oracle works to minimize the use of critical security maintenance, and to the extent reasonable, will work to provide 24 hours prior notice for any critical security maintenance requiring a service interruption outside of scheduled maintenance periods.

4.1.2 Data Center Migrations

Oracle may migrate Your Oracle Cloud Services deployed in data centers retained by Oracle between production data centers in the same Data Center Region as deemed necessary by Oracle or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days notice to You.

4.2 Software Versioning

4.2.1 Software Updates

Oracle requires all Oracle Cloud Services customers to keep the software versions of the Oracle Cloud Services current with the software versions that Oracle designates as supported releases for such Oracle Cloud Services. Software updates are required for the Oracle Cloud Services in order to maintain version currency. Oracle's obligations under these Delivery Policies (including the *Oracle Cloud Service Continuity Policy,* the *Oracle Cloud Service Level Agreement*, and the *Oracle Cloud Support Policy*) are dependent on You maintaining the currently supported versions of Your Oracle Cloud Services. Oracle is not responsible for performance, functionality, availability or security issues experienced with Oracle Cloud Services that may result from running earlier versions.

4.2.2 End of Life

Oracle will host and support only the supported releases of an Oracle Cloud Service. All other versions of the Oracle Cloud Service are considered as "End of Life" (EOL). You are required to complete the Oracle Cloud Services update to the latest version before the EOL of a given version. You acknowledge that failure to complete the update prior to the EOL of an Oracle Cloud Service version may result in an update automatically performed by Oracle or a suspension of the Oracle Cloud Services. In certain circumstances where an Oracle Cloud Service version reaches EOL and Oracle does not make available an updated version, Oracle may designate, and require You to transition to, a successor Oracle Cloud Service.

5. ORACLE CLOUD SUPPORT POLICY

The support described in this *Oracle Cloud Support Policy* applies only for Oracle Cloud Services and is provided by Oracle as part of such Oracle Cloud Services under Your order. Oracle may make available, and You may order for additional fees, additional support service offerings made available by Oracle for the Oracle Cloud Services.

5.1 Oracle Cloud Support Terms

5.1.1 Support Fees

The fees paid by You for the Oracle Cloud Services under Your order include the support described in this *Oracle Cloud Support Policy*. Additional fees are applicable for additional Oracle support services offerings purchased by You.

5.1.2 Support Period

Oracle Cloud support becomes available upon the Oracle Cloud Services start date and ends upon the expiration or termination of the Services (the "support period"). Oracle is not obligated to provide the support described in this Oracle Cloud Support Policy beyond the end of the support period.

5.1.3 Technical Contacts

Your technical contacts are the sole liaisons between You and Oracle for Oracle support for Oracle Cloud Services. Those technical contacts must have, at a minimum, initial basic service training and,

as needed, supplemental training appropriate for specific role or implementation phase, specialized service/product usage, and migration. Your technical contacts must be knowledgeable about the Oracle Cloud Services in order to help resolve system issues and to assist Oracle in analyzing and resolving service requests. When submitting a service request, Your technical contact should have a baseline understanding of the problem being encountered and an ability to reproduce the problem in order to assist Oracle in diagnosing and triaging the problem. To avoid interruptions in Oracle support for Oracle Cloud Services, You must notify Oracle whenever technical contact responsibilities are transferred to another individual.

5.1.4 Oracle Cloud Support

Oracle support for Oracle Cloud Services consists of:

- Diagnoses of problems or issues with the Oracle Cloud Services
- Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that those Oracle Cloud Services perform in all material respects as described in the associated Service Specifications
- Support during Change Management activities described in the *Oracle Cloud Change Management Policy* (see above)
- Assistance with technical service requests 24x7x365
- 24x7x365 access to a Cloud Customer Support Portal designated by Oracle and Live Telephone Support to log service requests
- Access to community forums
- Non-technical customer service assistance during normal Oracle business hours (8:00 to 17:00) local country time

5.2 Oracle Cloud Customer Support Systems

5.2.1 Oracle Cloud Customer Support Portal

Oracle provides support for the Oracle Cloud Service acquired by You, under an Order, through the Cloud Customer Support Portal (support portal) designated for that Oracle Cloud Service. While Oracle Cloud Support and the portals (including any portion of the Services they may provide) may be part of Your order, they are not an Oracle Cloud Service offering, and they may be delivered globally, with access to them governed by the Terms of Use posted on the applicable portal web sites, which terms of use are subject to change. Where such portals allow You to upload information, You are responsible for ensuring that You and Your Users do not submit any government-issued identification numbers or any health, financial, payment card, controlled unclassified information, or other sensitive personal information into such portals, unless otherwise expressly permitted by the terms of the support portal or Your applicable Cloud Services order. Access to the support portal is limited to Your designated technical contacts and other authorized users of the Oracle Cloud Services. Where applicable, the support portal provides support details to Your designated technical contacts to enable use of Oracle support for Oracle Cloud Services. Support notifications and alerts relevant to your service requests are posted in the support portal.

5.2.2 Live Telephone Support

Your technical contacts may access live telephone support via the phone numbers and contact information found on Oracle's support web site at https://www.oracle.com/support/contact.html.

5.3 Severity Definitions

Service requests for Cloud Services may be submitted by Your designated technical contacts via the support portal. The severity level of a service request is assigned based on inputs from You, and will be based on the following severity definitions:

5.3.1 Severity 1 (Critical Outage)

Your production use of the Oracle Cloud Services is stopped or so severely impacted that You cannot reasonably continue work. You experience a complete loss of service. The impacted operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- Data corrupted
- A critical documented function is not available
- Service hangs indefinitely, causing unacceptable or indefinite delays for resources or response
- Service crashes, and crashes repeatedly after restart attempts
- Security Incident with the potential to impact the confidentiality, integrity or availability of the service

Oracle will use reasonable efforts to respond to Severity 1 service requests within fifteen (15) minutes. Throughout the period during which Oracle is working to address a Severity 1 service request, You agree to make available Your technical contact 24x7. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, an approved action plan is in place or the Customer's 24x7 contact is no longer available. You must provide Oracle with a technical contact during this 24x7 period to assist with data gathering, testing, and applying fixes. You are required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

5.3.2 Severity 2 (Significant Impairment)

You experience a severe loss of service. Important features of the Oracle Cloud Services are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

5.3.3 Severity 3 (Technical Issue)

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

5.3.4 Severity 4 (General Guidance)

You request information, enhancement, or documentation clarification regarding the Oracle Cloud Services, but there is no impact on the operation of such service. You experience no loss of service.

5.4 Change to Service Request Severity Level

5.4.1 Initial Severity Level

At the time when the service request is created, Oracle will record an initial severity level of the service request based on the above severity definitions and/or Your inputs. Oracle's initial focus, upon creation of a service request, will be to resolve the issues underlying the service request. The severity level of a service request may be adjusted as described below.

5.4.2 Downgrade of Service Request Levels

As work on the underlying issue progresses, if the issue no longer warrants the severity level currently assigned based on its current impact on the operation of the applicable Oracle Cloud Service, then the severity level will be downgraded to the severity level that most appropriately reflects its current impact.

5.4.3 Upgrade of Service Request Levels

If, during the service request process, the issue warrants the assignment of a higher severity level than that currently assigned based on the current impact on the production operation of the applicable Oracle Cloud Service, then the severity level will be upgraded to the severity level that most appropriately reflects its current impact.

5.4.4 Adherence to Severity Level Definitions

You shall ensure that the assignment and adjustment of any severity level designation is accurate based on the current impact on the production operation of the applicable Oracle Cloud Service.

5.5 Service Request Escalation

For service requests that are escalated by You, the Oracle support analyst will engage the Oracle service request escalation manager who will be responsible for managing the escalation. The Oracle service request escalation manager will work with You to develop an action plan and allocate the appropriate Oracle resources. If the issue underlying the service request continues to remain unresolved, You may contact the Oracle service request escalation manager to review the service request and request that it be escalated to the next level within Oracle as required. To facilitate the resolution of an escalated service request, You are required to provide contacts within Your organization that are at the same level as that within Oracle to which the service request has been escalated.

6. ORACLE CLOUD SUSPENSION AND TERMINATION POLICY

6.1 Termination of Oracle Cloud Services

For a period of 60 days after the end of the Services Period for the Oracle Cloud Services or, if applicable, the 60 day period following Your termination of Cloud Services that You consume in a Pay as You Go model, following the end of their associated Services Period, Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content residing in the Oracle Cloud Services, or keep the service system accessible, for the purpose of data retrieval by You.

For free trials and pilots of Oracle Cloud Services, Oracle will make Your Content available for a period of 30 days following end of the trial or pilot. During this retrieval period, Oracle's Cloud Service Level Agreement does not apply and the service system may not be used for any production activities. Oracle has no obligation to retain Your Content after this retrieval period.

If You need assistance from Oracle to obtain access to or copies of Your Content, You must create a service request in the support portal.

Data retrieval and any related assistance by Oracle is not applicable for Oracle Cloud Services that do not store Your Content. You are responsible for ensuring that if those Oracle Cloud Services are dependent on separate Oracle Cloud Services (such as Storage Cloud Service or Database Cloud Services) for the storage of data, those separate Oracle Cloud Services must have a valid duration through the end of the terminating Oracle Cloud Service to enable data retrieval, or for otherwise taking appropriate action to back up or otherwise store separately Your Content while the production Oracle Cloud Services is still active prior to the end of the Services Period.

Following expiry of the retrieval period, Oracle will delete Your Content from the Oracle Cloud Services (unless otherwise required by applicable law).

For Oracle Cloud at Customer Services, You must make available for retrieval by Oracle any Oracle Cloud at Customer Service-related hardware components (including the gateway equipment) provided by Oracle in good working order and the same condition as at the start of the Oracle Cloud at Customer Services subject to reasonable wear and tear for appropriate use.

7 USE OF SERVICES

You are responsible for ensuring that access and use of acquired Oracle Cloud Services, and the benefit received from such Cloud Services, is only by and for Users in countries in accordance with Oracle's Global Trade Compliance policy described at https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html.