Overview

The Cloud Services described herein are provided under the terms of the agreement, ordering document, and these Delivery Policies. Oracle’s delivery of the services is conditioned on you 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, security, or availability of services provided during the Services Period.

Oracle Public Cloud Machine. Oracle Public Cloud Machine (“OPCM”) is an Oracle Cloud Service that is deployed at your data center or a third-party data center retained by you. Oracle will deliver to your data center certain hardware components, including remote gateway equipment, needed by Oracle to operate OPCM. You are responsible for providing adequate space, power, and cooling to deploy the Oracle hardware including the remote gateway, and for ensuring adequate network connectivity for Oracle Cloud Operations to access the service. Oracle is solely responsible for maintenance of the Oracle hardware components including remote gateway equipment.

1. Oracle Cloud Security Policy

1.1 Scope
Oracle provides reasonable and appropriate security measures designed to protect the Services Environment of the Oracle Cloud Services governed by these Delivery Policies. For the purpose of the Oracle Cloud Services ordered by you, “Services Environment” refers to the combination of hardware and software components, from the virtualization layer down to the physical security of the data center facilities in which the services operate, that are owned, licensed or managed by Oracle and to which Oracle grants you and Your Users access as part of the Cloud Services.

1.2 Customer Responsibilities
You are solely responsible for configuring, operating, maintaining, and securing the operating systems and other associated software of your Cloud Services including Your Applications. You are solely 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 routine archiving of Your Content. Oracle Cloud log-in credentials and private keys generated as part of the Cloud Services are for your internal use of the services only, and you may not sell, share, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your subcontractors who are Users of the Cloud Services and performing work on your behalf.

You are responsible for providing adequate network intrusion detection system and firewalls to ensure access to OPCM is restricted to approved users including restricting and segregating management networks from public access.

For OPCM, (a) you are responsible for providing adequate network intrusion detection systems and firewalls to ensure that access to OPCM is restricted to approved users including restricting and segregating management networks from public access, and (b) you are responsible for providing adequate network intrusion detection
systems and firewalls to ensure that access to OPCM is restricted to approved users including restricting and segregating management networks from public access.

2. Oracle Cloud Service Level Objective Policy

2.1 Service Availability Provisions
Commencing at Oracle’s activation of Customer’s Cloud Services, and provided that Customer remains in compliance with the terms of the ordering document (including the agreement) and meets Oracle’s recommended minimum technical configuration requirements for accessing and using the services from Customer’s network infrastructure and the Customer’s user work stations as set forth in the Cloud Service Program Documentation, Oracle works to meet the Service Level Objective in accordance with the terms set forth in this Policy.

2.2 Definition of Unplanned Downtime
For each month of the Services Period, Oracle will use commercially reasonable efforts to make the Cloud Services available with a Monthly Uptime Percentage as specified in the associated Service Description for the Oracle Cloud Service ordered by Customer (the “Service Commitment”).

“Unplanned Downtime” means any time during which the services are not available, but does not include any time during which the services or any services component are not available due to:

- A failure or degradation of performance or malfunction resulting from scripts, data, applications, equipment, infrastructure, software, penetration testing, performance testing, or monitoring agents directed or provided or performed by Customer
- Planned outages, scheduled or announced maintenance or maintenance windows, or outages initiated by Oracle at the request or direction of Customer or initiated by You for maintenance, activation of configurations, backups or other purposes that require the service to be temporarily taken offline
- Unavailability of management, auxiliary or administration services, including administration tools, reporting services, utilities, third party software components not within the sole control of Oracle, or other services supporting core transaction processing
- Outages occurring as a result of any actions or omissions taken by Oracle at the request or direction of Customer
- Outages resulting from Customer equipment or third party equipment or software components not within the sole control of Oracle
- Events resulting from an interruption or shut down of the services due to circumstances reasonably believed by Oracle to be a significant threat to the normal operation of the services, the operating infrastructure, the facility from which the services are provided, access to, or the integrity of Customer data (e.g., a hacker or a virus attack)
- Outages due to system administration, commands, or file transfers performed by Customer users or representatives
- Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and Oracle’s other vendors), and other force majeure events
- Inability to access the services or outages caused by Customer’s conduct, including negligence or breach of Customer material obligations under the agreement, or by other circumstances outside of Oracle’s control
- Lack of availability or untimely response time of Customer to respond to incidents that require Customer participation for source identification and/or resolution, including meeting Customer responsibilities for any services
- Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to Customer conduct or circumstances outside of Oracle’s control