Oracle Maps Cloud Service Enterprise Hosting and Delivery Policies

Effective Date: October 1, 2015
Version 1.0

Unless otherwise stated, these Oracle Maps Cloud Service Enterprise Hosting and Delivery Policies (the "Delivery Policies") describe 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 the ordering document. Capitalized terms that are not otherwise defined in this document shall have the meaning ascribed to them in the relevant Oracle Agreement, ordering document or policy.

Overview and Table of Contents

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 Cloud Services provided during the Services Period.

Access
Oracle provides Cloud Services from Oracle owned or leased data center space. Oracle defines the services' network and systems architecture, hardware and software requirements.

Hours of Operation
The Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during system maintenance periods and technology upgrades and as otherwise set forth in the agreement, the ordering document and these Delivery Policies.

The Hosting and Delivery Policies include the following:

1. Oracle Cloud Security Policy
2. Oracle Cloud System Resiliency Policy
3. Oracle Cloud Disaster Recovery Service Policy
4. Oracle Cloud Service Level Objective Policy
5. Oracle Cloud Change Management Policy

1. Oracle Cloud Security Policy

1.1 Network Security Management

1.1.1 Network Controls

Network controls implemented for Oracle Cloud Services address the protection and control of data during its transmission from Customer's system to the Oracle hosted system. The network security infrastructure is designed to secure the servers from a network-based attack. Redundant, managed firewalls, using stateful packet inspection, provide barriers between tiers of the architecture. Traffic is filtered, and only valid connections are allowed through into the network demilitarized zone. Traffic within each tier is restricted and controlled for security purposes.

1.1.2 Network Intrusion Detection/Prevention System

Oracle Cloud Services utilize Network Intrusion Detection Systems (nIDS) to protect the environment. nIDS sensors are deployed in either IPS (Intrusion Prevention Mode) or IDS (Intrusion Detection Mode) on the network, to monitor and block suspicious network traffic from reaching the internal network. nIDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365.

1.1.3 Network Vulnerability Assessments

Oracle Cloud Services utilize network vulnerability assessment tools to identify security threats and vulnerabilities. Formal procedures are in place to assess, validate, prioritize, and remediate identified issues. Oracle subscribes to vulnerability notification systems to stay apprised of security incidents, advisories, and other related information. Oracle takes actions on the notification of a threat or risk once confirmed that a valid risk exists, that the recommended changes are applicable to service environments, and the changes will not otherwise adversely affect the services.

1.1.4 Anti-Virus Controls

Oracle Cloud employs anti-virus software to scan uploaded files. Viruses that are detected are removed (or quarantined) automatically, and an alert is automatically generated which initiates Oracle's incident response process. Virus definitions are updated daily.

1.1.5 Configuration Control/Audit

Oracle Cloud uses a centralized system for managing the access and integrity of network device configurations. Change controls are in place to ensure only approved changes are applied. Regular audits are also performed to confirm compliance with security and operational procedures.

1.2 System Hardening

Oracle employs standardized system hardening practices across Oracle Cloud devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging.

1.3 Physical Security Safeguards

Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and co-locations/datacenters currently include, for instance:

- Physical access requires authorization and is monitored.
- Everyone must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed when on the premises
- 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 all Oracle Cloud data centers, which currently include safeguards such as:

- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent vehicles from unauthorized entry
- Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management

1.4 System Access Control & Password Management

Access to Oracle Cloud systems is controlled by restricting access to only authorized personnel. Oracle enforces strong password policies on infrastructure components and cloud management systems used to operate the Oracle Cloud environment. This includes requiring a minimum password length, password complexity, and regular password changes. Strong passwords or multi-factor authentication are used throughout the infrastructure to reduce the risk of intruders gaining access through exploitation of user accounts.

1.5 Review of Access Rights

Network and operating system accounts for Oracle employees are reviewed regularly to ensure appropriate

employee access levels. In the event of employee terminations, Oracle takes prompt actions to terminate network, telephony, and physical access for such former employees.

1.6 Security-Related Maintenance

Oracle performs security related change management and maintenance as defined and described in the Oracle Cloud Change Management Policy. For any security patch bundle that Oracle will deploy for designated Oracle Programs, Oracle will apply and test the security patch bundle on a stage environment of the applicable Cloud Service. Oracle will apply the security patch bundle to the production environment of the Cloud Service after Oracle successfully completes testing on the stage environment.

1.7 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 services. The OSSA program is described at http://www.oracle.com/us/support/assurance/overview/index.html.

2. Oracle Cloud System Resiliency Policy

2.1 Oracle Cloud Services High Availability Strategy

For business continuity in the event of an incident affecting Oracle Cloud Services, Oracle deploys the services on resilient computing infrastructure. Oracle's production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis as described below.

2.2 Redundant Power

The infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.

2.3 Redundant Network Infrastructure

Network designs include redundant circuits from different carriers, firewall pairs, switch pairs, and load balancer pairs.

2.4 Redundant Database Servers

Databases are configured to distribute workload across multiple physical servers. High availability is achieved through clustering and replication.

2.5 Redundant Storage

Oracle Cloud services data resides in redundant storage configurations with protection from individual disk or array failure.

2.6 Oracle Cloud Services Backup Strategy

In support of Oracle's Cloud Disaster Recovery practices (see Section 3 below), Oracle periodically makes backups of production data in Customer's Cloud Service for Oracle's sole use to minimize data loss in the event of a disaster. Database backups are stored at the primary site used to provide the Oracle Cloud Services, as well as at an alternate location for redundancy purposes. A backup is retained online and/or offline for a period of at least 60 days after the date that the backup is made.

3. Oracle Cloud Disaster Recovery Service Policy

3.1 Scope

Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster,

as declared by Oracle, that leads to loss of a data center and corresponding service unavailability.

For the purposes of this Policy, a “disaster” means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the Oracle Cloud Services such that the environments at the primary site are not available.

3.2 System Resilience

Oracle Cloud Services maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Oracle designs its cloud services using principles of redundancy and fault-tolerance with a goal of fault-tolerance of a single node hardware failure.

Oracle Cloud Services provide an infrastructure that incorporates a comprehensive data backup strategy. The Oracle Cloud includes redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases.

Oracle has two separate data centers that function as primary and secondary sites for Oracle Cloud Services. Production standby (secondary site) environment will reside in a data center separate from the primary site. Oracle will commence the disaster recovery plan under this Policy upon its declaration of a disaster, and will target to recover the production data and use reasonable efforts to re-establish the production environment at the secondary site.

3.3 Disaster Recovery

Oracle provides for the recovery and reconstitution of its production Cloud Services to the most recent available state following a disaster.

Oracle has established alternate processing sites to accommodate full operating capability in the event of loss of service at a primary facility. Oracle maintains a Disaster Recovery Plan that describes recovery procedures.

Disaster recovery operations apply to the physical loss of infrastructure at Oracle facilities. Oracle reserves the right to determine when to activate the Disaster Recovery Plan. During the execution of the Disaster Recovery Plan, Oracle provides regular status updates to Customers.

3.3.1 Recovery Time Objective

Recovery time objective (RTO) is Oracle’s objective for the maximum period of time between Oracle’s decision to activate the recovery processes under this Policy to failover the service to the secondary site due to a declared disaster, and the point at which Customer can resume production operations in the standby production environment. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO is 12 hours from the declaration of a disaster.

3.4 Approvals and Reviews

This Policy and the corresponding Disaster Recovery Plan is reviewed annually. The Plan is revised during the review process to incorporate problem resolutions and process improvements.

3.5 Service Restoration

This Policy identifies the purpose and scope of the Disaster Recovery Plan, the roles and responsibilities, management commitment, coordination among organizational entities, and compliance. The plan documents the procedures for recovering a Cloud Service in the event of a disaster.

Oracle is committed to minimizing down time due to any disasters or equipment failures. As part of this commitment, Oracle has a corporate business disaster recovery plan for a timely recovery and restoration of Oracle operations.

3.6 Disaster Recovery Plan Objectives

The following are the objectives of Oracle's Disaster Recovery Plan for Oracle Cloud Services:

- In an emergency, Oracle's top priority and objective is human health and safety.
- Maximize the effectiveness of contingency operations through the established Disaster Recovery Plan that consists of the following phases:
    - Phase 1 - Disaster Recovery Launch Authorization phase - to detect service disruption or outage at the primary site, determine the extent of the damage and activate the plan.
    - Phase 2 - Recovery phase - to restore temporary IT operations at the secondary site.
    - Phase 3 - Reconstitution phase - to restore processing capabilities and resume operations at the primary site.
- Identify the activities, resources, and procedures to carry out processing requirements during prolonged interruptions.
- Assign responsibilities to designated personnel and provide guidance for recovery, during prolonged periods of interruption.
- Ensure coordination with other personnel responsible for disaster recovery planning strategies. Ensure coordination with external points of contact and vendors and execution of this plan.

3.7 Plan Testing

The Cloud Services Disaster Recovery Plan is tested, as a live exercise or a table-top test, on an annual basis. The tests are used for training hosting personnel and are coordinated with all personnel responsible for contingency planning and execution. The tests verify that online backups can be recovered and the procedures for shifting a service to the alternate processing site are adequate and effective. Test plans are developed in accordance with NIST 800-34. Results of the testing are used to improve the process and initiate corrective actions.

4. Oracle Cloud Service Level Objective Policy

4.1 Target System Availability Level of Oracle Cloud Service

Oracle works to meet a Target System Availability Level of 99.5% of the production service, for the measurement period of one calendar month.

4.2 Definition of Availability and Unplanned Downtime

"Availability" or "Available" means Customer is able to use the Oracle Cloud Services, subject to the following provisions. "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:

- Planned outages, scheduled and announced maintenance or maintenance windows, or outages initiated by Oracle for maintenance, activation of configurations, backups or other purposes that require the service to be temporarily taken offline;
- 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 malware attack);
- 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;
- 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.

4.3 Measurement of Availability

Following the end of each calendar month of the Services Period under an ordering document, Oracle measures the "System Availability Level" over the immediately preceding month. Oracle measures the System Availability

Level by dividing the difference between the total number of minutes in the monthly measurement period and any Unplanned Downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

4.4 Monitoring

Oracle uses a variety of software tools to monitor (i) the availability and performance production services environment and (ii) the operation of infrastructure and network components.

4.4.1 Monitored Components

Oracle monitors the service infrastructure, and currently generates alerts for CPU, memory, storage, database, network components, and transactions. Oracle's Operations staff attends to any automated warnings and alerts associated with deviations of the environment from Oracle defined monitoring thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

5. Oracle Cloud Change Management Policy

5.1 Oracle Cloud Change Management and Maintenance

Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the Oracle Cloud. Oracle follows formal change management procedures to provide the necessary review, testing, and approval of changes prior to application in the Oracle Cloud production environment.

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

Oracle reserves specific maintenance periods for changes that may require the Cloud Service to be unavailable during the maintenance period. Oracle works to ensure that change management procedures are conducted during scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements. Oracle will work to provide prior notice of modifications to the standard maintenance period schedule.

For changes that are expected to cause service interruption, Oracle will work to provide prior notice of the anticipated impact. The durations of the maintenance periods for planned maintenance are not included in the calculation of Unplanned Downtime minutes in the monthly measurement period for System Availability Level (see "Oracle Cloud Service Level Objective Policy"). 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.

5.1.1 Emergency Maintenance

Oracle may periodically be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the production environment. Emergency maintenance may include program patching and/or core system maintenance as required. Oracle works to minimize the use of emergency maintenance and will work to provide 24 hours prior notice as of any emergency maintenance requiring a service interruption.

5.1.2 Major Maintenance Changes

To help ensure continuous stability, availability, security and performance of the Cloud Services, Oracle reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control, no more than twice per calendar year. Each such change event is considered scheduled maintenance and may cause the Cloud Services to be unavailable for up to 24 hours. Each such change event is targeted to occur at the same time as the scheduled maintenance period. Oracle will work to provide up to 60 days prior notice of the anticipated unavailability.

5.2 Software and Data Versioning

5.2.1 Software Upgrades and Updates

Oracle Maps Cloud Service is based on data products from third party suppliers. Oracle works to update the map and map-related content on a regular basis based on the availability of data from the supplier. This may vary based on geographic region or content type. The data used in Oracle Maps Cloud Service is provided "as is" subject to the Supplier Licenses and Terms of Use. Use of the Oracle Maps Cloud Service requires all customers to keep the software versions of applications and Oracle Cloud Services that access this service current with the software versions that Oracle designates as generally available (GA). Oracle is not responsible for performance or security issues encountered with the Cloud Services that may result from running earlier versions.

5.2.2 End of Life

Oracle Maps Cloud Service is subject to the following End of Life Policy. Oracle will continue to support Oracle Maps Cloud Service, at a minimum, for the duration of the subscription term. In certain circumstances where a Cloud Service version reaches EOL and Oracle does not make available an upgraded version, Oracle may designate, and require Customers to transition to, a successor cloud service. Oracle makes commercially reasonable efforts to post notices of such EOL one quarter in advance of the EOL and reserves the right to deprecate, modify, or remove features from any new version without prior notice.

5.2.3 Deprecated Features

A deprecated feature is a feature that appears in prior or existing versions of the Cloud Service and is still supported as part of the service, but for which Oracle has given notification that the feature will be removed from future versions. Oracle makes commercially reasonable efforts to post notices of feature deprecations one quarter in advance of their removal and reserves the right to deprecate, modify, or remove features from any new version without prior notice.