Oracle Cloud-SaaS Hosting and Delivery Policies

Effective Date: December 1, 2012

Unless otherwise stated, these Oracle Cloud Hosting and Delivery Policies (the "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 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 or availability of 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. Oracle may access your services environment to perform the Cloud Services including the provision of service support.

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.

These Cloud Hosting and Delivery Policies include the following:

1. Oracle Cloud Security Policy
2. Oracle Cloud Service Level Objective Policy
3. Oracle Cloud Change Management Policy
4. Oracle Cloud Support Policy
5. Oracle Cloud Suspension and Termination Policy

1. Oracle Cloud Security Policy

1.1 User Encryption for External Connections

Customer access to the system is through the Internet. Where SSL encryption technologies are used, SSL connections are negotiated for at least 128 bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. It is recommended that the latest available browsers certified for Oracle applications, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled applications. The list of certified browsers for each version of Oracle applications can be found on the My Oracle Support portal. In some cases, a third-party site used with cloud services and not under the control of Oracle may force a non-encrypted connection. For those Cloud Services that provide integration with third-party sites (e.g., Facebook) where HTTP connections are permitted by Oracle and the third-party site, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.2 Network Access Control

Oracle Cloud operations teams access customer environments through a segregated network connection, which is dedicated to environment access control and isolated from Oracle's internal corporate network traffic.

Authentication, authorization, and accounting are implemented through standard security mechanisms designed to ensure that only approved operations and support engineers have access to the systems.

1.3 Network Bandwidth and Latency

Oracle is not responsible for Customer's network connections or for conditions or problems arising from or related to Customer's network connections (e.g., bandwidth issues, excessive latency, network outages), or caused by the Internet. Oracle monitors its own networks and will notify customers of any internal issues that may impact availability.

1.4 Firewalls

Utilized to control access between the Internet and Oracle Cloud Services by allowing only authorized traffic. Oracle managed firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address in order to identify authorized sources, destinations, and traffic types.

1.5 System Hardening

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

1.6 Physical Security Safeguards

Oracle provides secure computing facilities for production cloud infrastructure which include:

- 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
- 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

1.7 System Access Control & Password Management

Access to Cloud systems is controlled by restricting access to only authorized personnel. Oracle enforces password policies on all infrastructure components and cloud management systems used to operate the Oracle Cloud environment.

System access controls include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users'. Customer is responsible for all end user administration within the application. Oracle does not manage the Customer's End User accounts. Customer may configure the applications and additional built-in security features to meet its business or compliance needs.

1.8 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. Customer is responsible for managing and reviewing access for its own employee accounts.

1.9 Data Management / Protection

During the use of Oracle Cloud services, Oracle Cloud customers maintain control over and responsibility for their data residing in their environment. Oracle Cloud services provide a variety of configurable information protection

services as part of the subscribed service. Customer data is data uploaded or generated for use within the Oracle Cloud Services.

1.9.1 Physical Media in Transit

Designated Oracle personnel handle media and prepare it for transportation according to defined procedures and only as required. Digital media is logged, encrypted, securely transported, and as necessary for backup archiving vaulted by a third-party off-site vendor. Vendors are contractually obligated to comply with Oracle-defined terms for media protection.

1.9.2 Data Disposal

Upon termination of services (as described in the Oracle Cloud Suspension and Termination Policy) or at Customer's request, Oracle will delete environments or application data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the environments or data.

1.9.3 Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to or handling of customer data whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Global Information Security (GIS) organization is informed of such incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those incidents. GIS will work with Customer, the appropriate technical teams, and law enforcement where necessary to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of Customer's environment, and to establish root causes and remediation steps. Operations staff has documented procedures for addressing incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain of custody practices.

If Oracle determines that Customer's data has been misappropriated, Oracle will promptly report such misappropriation to Customer unless prohibited by law.

1.9.4 Data Privacy

The Oracle Data Processing Agreement incorporated into the ordering document, as well as Oracle's Services Privacy Policy, describes Oracle's treatment of data that resides on Oracle, customer or third-party systems (including personally identifiable information or "PII") to which Oracle may be provided access in connection with the provision of hosted services. The Oracle Services Privacy Policy is available at http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html

2. Oracle Cloud Service Level Objective Policy

2.1 Service Availability Provisions

Commencing at Oracle's activation of Customer's production environment, 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 Target Service Availability Level in accordance with the terms set forth in this Policy.

2.2 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, commencing at Oracle's activation of the production environment.

2.3 Definition of Availability and Unplanned Downtime

"Availability" or "Available" means Customer is able to log in and access the OLTP or transactional portion of 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:

- 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 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, 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 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

2.4 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.

2.5 Monitoring

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

2.6 Customer Monitoring & Testing Tools

Due to potential adverse impact on service performance and availability, Customer may not use its own monitoring or testing tools (including automated user interfaces and web service calls to any Oracle Cloud Service) to directly or indirectly seek to measure the availability, performance, or security of any application or feature of or service component within the services or environment. Exceptions to this are the Oracle Database Cloud Service and Oracle Java Cloud Service or if otherwise expressly permitted in the ordering document. Oracle reserves the right to remove or disable access to any tools that violate the foregoing restrictions without any liability to Customer.

2.7 Customer Workloads

Customer may not make significant workload changes beyond the amount permitted under the entitlements provided under ordering document.

2.8 Automated Workloads

Customer may not use nor authorize the use of data scraping tools or technologies to collect data available through the Oracle Cloud Service user interface or via web service calls without the express written permission of Oracle. Oracle reserves the right to require Customer's proposed data scraping tools to be validated and tested by Oracle prior to use in production and to be subsequently validated and tested annual. Oracle may require that a written statement of work be executed to perform such testing and validation work.

3. Oracle Cloud Change Management Policy

3.1 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 Services. 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

Change Management procedures include management of regular and ongoing application upgrades and updates, coordinated customer specific changes where required, and system and service maintenance. Oracle works to architect cloud services to avoid service interruption where possible.

Where an anticipated change will require the application service to be unavailable during the change maintenance period, Oracle will work to provide prior notice of the anticipated impact. The duration of the maintenance periods for planned maintenance are not included in the calculation of available minutes in the monthly measurement period for System Availability Level (see "Oracle Cloud Service Level Objective Policy"). Oracle intends to minimize the use of these reserved maintenance periods and minimize the duration of maintenances causing unavailability of service.

3.1.1 Application Upgrades and Updates

Oracle requires that the application versions of Oracle Cloud Services be kept current with the application versions that Oracle designates as generally available (GA) to its commercial customers.

Oracle is not responsible for performance or security issues encountered with the Cloud Services that may result from running earlier application versions. Application updates follow release of every application GA and are required to maintain application version currency. Application upgrades and updates will be applied to all target customers by Oracle in accordance with Oracle's target deployment schedule.

Oracle will provide prior notice for application upgrades and updates that involve service interruption.

3.1.2 Core System Maintenance

Core system maintenance involves changes to hardware, network systems, security systems, operating systems, storage systems or general supporting software of the cloud infrastructure. Core system maintenance requiring a service interruption is performed every 1st and 3rd Friday of the month.

The scheduled service period for core system maintenance requiring service interruption is on the 1st and 3rd Friday of the month and will be scheduled by Oracle between 21:00-06:00 data center local time.

Oracle may elect to not schedule a core system maintenance event.

3.1.3 Routine Infrastructure Maintenance

Oracle manages routine infrastructure maintenance for the purpose of providing environment currency, capacity, and stability. Routine maintenance is not expected to result in a service interruption.

3.1.4 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 application patching and/or core system maintenance as required. Oracle works to minimize the use of emergency maintenance and will provide as much notice as reasonable under the circumstances as to any emergency maintenance requiring a service interruption.

3.1.5 Major Maintenance Changes

To 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 planned maintenance and may cause the Cloud Services to be unavailable for up to 24 hours.

3.2 Deprecated Features

A deprecated feature is a feature that appears in prior or existing versions of the 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.

4. Oracle Cloud Support Policy

The support described in this Cloud Support Policy applies only for Oracle Cloud Services and is provided by Oracle as part of such services under the ordering document. Customer may purchase additional services for Oracle Cloud via other Oracle support service offerings that are designated by Oracle for Cloud Services.

4.1 Oracle Cloud Support Terms

4.1.1 Support fees

The fees paid by Customer for the Oracle Cloud Services offering under the ordering document include the support described in this Oracle Cloud Support Policy. Additional fees are applicable for additional Oracle support services offerings purchased by Customer.

4.1.2 Support period

Oracle Cloud support is effective upon the effective date specified in the ordering document and ends upon the expiration or termination of the service under such ordering document (the "support period"). Oracle is not obligated to provide the support described in this Cloud Support Policy beyond the end of the support period.

4.1.3 Technical contacts

Customer's technical contacts are the sole liaisons between Customer and Oracle for Oracle Cloud support services. Such technical contacts must have, at minimum, initial basic training for Oracle Cloud and, as needed, supplemental training appropriate for specific role or implementation phase, specialized service/product usage, and/or migration. Customer's technical contacts must be knowledgeable about the Oracle Cloud service offerings and the Oracle environment in order to help resolve system issues and to assist Oracle in analyzing and resolving service requests. When submitting a Service Request, Customer's 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 support services, Customer must notify Oracle whenever technical contact responsibilities are transferred to another individual.

4.1.4 Oracle Cloud Support

Support Services for Oracle Cloud consists of:

- Diagnosis 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 they perform in all material respects as described in the associated Program Documentation

- Support during Change Management activities described in the Oracle Cloud Change Management Policy
- Assistance with Technical Service Requests 24 hours per day, 7 days a week
- 24 x 7 access to My Oracle Support, Oracle Cloud Customer Portal 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 time.

4.2 Oracle Cloud Customer Support Systems

4.2.1 My Oracle Support

Oracle provides customer support for Oracle Cloud Services through its My Oracle Support web site. Access to My Oracle Support is governed by the Terms of Use posted on the My Oracle Support web site, which are subject to change. A copy of these terms is available upon request. Access to My Oracle Support is limited to Customer's designated technical contacts for Cloud Services. Access to My Oracle Support is included as part of the support service for the Oracle Cloud offerings acquired by Customer under the ordering document.

4.2.2 Oracle Cloud Customer Portal

Oracle Cloud Customer Portal provides the Customer Service Identifier (CSI) and other support details to Customer's designated technical contacts to enable use of Oracle Cloud support. All customer relevant service notifications and alerts are posted on this portal.

4.2.3 Live Telephone Support

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

4.3 Security Practices for Oracle Cloud Support

Oracle is deeply committed to the security of Oracle Cloud Services support. In providing Oracle Cloud Services support, Oracle will adhere to the Oracle Cloud Security Policy set forth in the Oracle Cloud Hosting and Delivery Policies.

Oracle will also provide Oracle Cloud Services support in accordance with Oracle's services privacy policy, available at http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html .

4.4 Severity Definitions

Service requests for Oracle Cloud Services may be submitted by Customer's designated technical contacts via the Oracle Cloud Customer Support Systems noted in Section 4.2 of this Policy. The severity level of a service request submitted by Customer is selected by both Customer and Oracle, and must be based on the following severity definitions:

Severity 1

Customer's production use of the Oracle Cloud Service is stopped or so severely impacted that Customer cannot reasonably continue work. Customer experiences 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

Oracle will use reasonable efforts to respond to Severity 1 service requests within one (1) hour. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, or as long as useful progress can be made. Customer must provide Oracle with a contact during this 24x7 period to assist with

data gathering, testing, and applying fixes. Customer is required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2
Customer experiences 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.

Severity 3
Customer experiences a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Severity 4
Customer requests information, enhancement, or documentation clarification regarding the Oracle Cloud Service, but there is no impact on the operation of such service. Customer experiences no loss of service.

4.5 Change to Service Request Severity Level

4.5.1 Initial Severity Level

At the time Oracle accepts a service request, Oracle will record an initial severity level of the service request based on the above severity definitions. Oracle's initial focus, upon acceptance 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.

4.5.2 Downgrade of Service Request Levels: If, during the service request process, the issue no longer warrants the severity level currently assigned based on its current impact on the production 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.

4.5.3 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.

4.5.4 Adherence to Severity Levels definitions: Customer 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. Customer acknowledges that Oracle is not responsible for any failure to meet performance standards caused by Customer's misuse or misassignment of severity level designations.

4.6 Service Request Escalation

For service requests that are escalated, 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 Customer to develop an action plan and allocate the appropriate Oracle resources. If the issue underlying the service request continues to remain unresolved, Customer 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, Customer is required to provide contacts within Customer's organization that are at the same level as that within Oracle to which the service request has been escalated.

4.7 Policy Exceptions

Customer questions or requests for an exception to the Oracle Cloud Hosting and Delivery Policies must be made via a service request with My Oracle Support.

5. Oracle Cloud Suspension and Termination Policy

5.1 Termination of Cloud Services

5.1.1 Termination of Cloud Services

For a period of up to 60 days after the termination or expiration of production services under the ordering document, Oracle will preserve an original or copy of Customer's applicable services or customer data as it existed in the Customer's environment on the date of termination. Oracle has no obligation to retain the data for customer purposes after this 60 day post termination period. Oracle Customer Support Identifiers (CSIs) are terminated at the end of the 60 day period.

5.1.2 Termination of Trial Environments

Upon the expiration of a trial, the service is terminated with no archiving of data. To avoid loss of data, Customer must work with authorized Oracle representatives to enter into an extension of the trial period before its expiration.

5.1.3 Termination of Pilot Environments

Pilots of Oracle Cloud Services adhere to the same service termination policy as normal production environments.

5.1.4 Customer Assistance at Termination

At service termination, if Customer needs assistance from Oracle**,** Customer must create a service request in My Oracle Support.

5.1.5 Secure File Transfers

As part of the service termination process, Oracle provides a method for secure file transfer of Customer data. The secure file transfer functionality has a separate directory and mapped file volume for each customer for unique data access. Each directory may only be viewed by the designated Customer.

Access to the file transfer site is by a user account that is provided to Customer as part of the termination process. Data transmission is provided via secure protocols.

5.2 Suspension Due to Violation

If Oracle detects violation, or is contacted about a violation of, Oracle Cloud Services terms and conditions or acceptable use policy, Oracle will assign an investigating agent. The investigating agent may take actions including but not limited to suspension of user account access, suspension of administrator account access, or suspension of the environment until the issues are resolved.

Oracle will use reasonable efforts to restore Customer's services promptly after Oracle determines, in its reasonable discretion, that the issues have been resolved or the situation has been cured.