Oracle Cloud Hosting and Delivery Policies

Effective Date: December 1, 2014
Version 1.4

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, 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. 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

1.1 User Encryption for External Connections

Customer access to the system is through the Internet. SSL encryption technology is available for Oracle Cloud Service access. 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. SSL is implemented or configurable for all web-based SSL 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 version of Oracle programs can be found on the Cloud Customer Support Portal designated by Oracle for the specific service ordered (e.g., 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. In some cases, a third party site (such as Facebook) that Customer wishes to integrate with the Cloud Service may not accept an encrypted connection. For 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.

1.2 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 Anti-Virus Controls

Oracle Cloud employs industry standard 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.

1.5 Firewalls

Oracle Cloud Services utilize firewalls 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, as appropriate, in order to identify authorized sources, destinations, and traffic types.

1.6 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.

1.7 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

1.8 System Access Control & Password Management

Access to Cloud systems is controlled by restricting access to only authorized personnel. Oracle enforces password policies on 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 program. Oracle does not manage the Customer's End User accounts. Customer may configure the programs and additional built-in security features.

1.9 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.

1.10 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 makes generally available 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.

1.11 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.

1.11.1 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.

1.11.2 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 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.

1.11.3 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. When Oracle's Global Information Security (GIS) organization is informed of such incidents, GIS defines escalation paths and response teams to address those incidents, depending on the nature of the activity. 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 the 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 report such misappropriation to Customer within three business days of making such determination, unless prohibited by law.

1.11.4 Data Privacy

Oracle's *Data Processing Agreement for Oracle Cloud Services* ("Data Processing Agreement), and the *Oracle Services Privacy Policy,* describe Oracle's treatment of data that resides on Oracle systems (including personally identifiable information or "PII") to which Oracle may be provided access in connection with the provision of Cloud Services. The Data Processing Agreement specifically describes Oracle's and Customer's respective roles for the processing and control of personal data that Customer provides to Oracle as part of the Cloud Services. These documents are available at:

- *Oracle Services Privacy Policy*: http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html

- *Data Processing Agreement for Oracle Cloud Services*: http://www.oracle.com/dataprocessingagreement

1.12 Regulatory Compliance

The Oracle Cloud services are aligned with ISO (International Organization for Standardization) 27001:2013 security controls.

The ISO security framework includes a comprehensive set of security controls that are used as a baseline for the operational and security controls utilized to manage and secure the Oracle Cloud Service, but this does not include ISO 27001 certification.

The internal controls of Oracle Cloud Services are subject to periodic testing by independent third party audit organizations. Such audits may be based on the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization ("SSAE 16"), the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization ("ISAE 3402"), or such other third party auditing standard or procedure applicable to the specific Oracle Cloud Service. Audit reports of Oracle Cloud Services are periodically published by Oracle's third party auditors, although reports may not be available for all services or at all times. Customer may request to receive a copy of the current published audit report available for a particular Oracle Cloud Service.

The audit reports of Oracle Cloud Services, and the information they contain, are Oracle confidential information, and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to Oracle Cloud Services and are provided without any warranty.

Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud Service. Customer must make Oracle aware of any technical requirements that result from its regulatory obligations prior to contract signing. Some Oracle Cloud services are certified to PCI DSS or FISMA/NIST standards and additional certifications and adherence to specific regulatory frameworks within the Oracle Cloud Service may be available for additional fees. Customer must not provide Oracle with health, payment card or other sensitive personal information that requires specific regulatory, legal or industry data security obligations for the processing of such data; however, where available for certain Cloud Services, Oracle may offer for purchase by Cloud Customers additional services designed for the processing of regulated data within the services environment. Note that such additional services are not available for all Cloud Services.

Oracle understands that some Customers may have regulatory audit requirements and Oracle will cooperate with Customer as described in the Data Processing Agreement in those cases.

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 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 Backup Strategy

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. Oracle typically does not update, insert, delete or restore Customer data on behalf of Customer. However, on an exception basis and subject to written approval and additional fees, Oracle may assist Customer to restore data which Customer may have lost as a result of their own actions.

3. Oracle Cloud Service Level Objective Policy

3.1 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. In these Delivery Policies, references to the term "production" mean (i) in the context of Oracle Cloud Software as a Service offerings, the production instances of such services, or (ii) in the context of Oracle Cloud Platform as a Service offerings, the development instances of such services.

3.2 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.

3.3 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 and 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, 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 malware 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.

3.4 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.

3.5 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.

3.5.1 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 program or feature of or service component within the services or environment. Oracle reserves the right to remove or disable access to any tools that violate the foregoing restrictions without any liability to Customer.

3.5.2 Customer Workloads

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

3.5.3 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.

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 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, upgrades and updates, and Customer specific changes. Oracle Cloud Change Management procedures are designed to minimize service interruption.

For Customer-specific changes and Upgrades, where possible, Oracle will work to coordinate the maintenance periods with Customer. 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.

4.1.1 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.

4.1.2 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 planned 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 either the core system maintenance or the program upgrade window. Oracle will work to provide up to 60 days prior notice of the anticipated unavailability.

4.2 Software Versioning

4.2.1 Software Upgrades and Updates

Oracle requires all Cloud Services Customers to keep the software versions of the Oracle Cloud Services current with the software versions that Oracle designates as generally available (GA). For Cloud Services that support multiple versions, Oracle typically designates the current and immediate previous version as GA versions. Oracle may provide notification regarding the GA release of specific Cloud Services on the support portal or within the Service Specifications for the Cloud Services. Software updates will follow the release of every GA release and are required to maintain version currency. Oracle Cloud Hosting and Delivery Policies, such as the Service Levels Objective Policy and the Cloud Support Policy, are dependent on Customer maintaining GA version currency. Oracle is not responsible for performance or security issues encountered with the Cloud Services that may result from running earlier versions.

4.2.2 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.

5. 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.

5.1 Oracle Cloud Support Terms

5.1.1 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.

5.1.2 Support period

Oracle Cloud support becomes available upon the service start date and ends upon the expiration or termination of the Cloud 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.

5.1.3 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.

5.1.4 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 a Cloud Customer Support Portal designated by Oracle (e.g., My Oracle Support) 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.

5.2 Oracle Cloud Customer Support Systems

5.2.1 Cloud Customer Support Portal

As part of the Oracle Cloud offering acquired by Customer under the ordering document, Oracle provides Customer Support for the Cloud Service through the Cloud Customer Support Portal designated for that Cloud Service. Access to the applicable Cloud Customer Support Portal is governed by the Terms of Use posted on the designated support web site, which are subject to change. A copy of these terms is available upon request. Access to the Cloud Customer Support Portal is limited to Customer's designated technical contacts and other authorized users of the Cloud Services. Where applicable, the Oracle Cloud Customer Support Portal provides 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.

5.2.2 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 or such other address designated by Oracle for the applicable Cloud Services ordered.

5.3 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 5.2 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.

5.4 Change to Service Request Severity Level

5.4.1 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.

5.4.2 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.

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 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 mis-assignment of severity level designations.

5.5 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.

5.6 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 the Cloud Customer Support Portal applicable to the service (e.g., My Oracle Support).

6. Oracle Cloud Suspension and Termination Policy

6.1 Termination of Cloud Services

6.1.1 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 make available Customer production data for the purpose of retrieval by Customer. 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.

6.1.2 Termination of Pilot Environments

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

6.1.3 Customer Assistance at Termination

At service termination, if Customer needs assistance from Oracle to obtain access to Oracle's secure server in order to retrieve its production data**,** Customer must create a service request in the Cloud Customer Support Portal applicable to the service (e.g., My Oracle Support).

6.1.4 Secure Data Transfers

As part of the service termination process, Oracle makes secured protocols available by which designated Customer users can transfer Customer data from the service.

6.2 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.

Appendix A – Oracle Eloqua Marketing Cloud Service

This appendix applies to the Oracle Eloqua Marketing Cloud Service Cloud Services and sets forth modifications to the Oracle Cloud Hosting and Delivery Policies, as follows:

3.3 Definition of Availability and Unplanned Downtime

The following additional exclusions apply to the Oracle Eloqua Marketing Cloud Service:

(i) any problems resulting from Customer combining or merging the Oracle Eloqua Marketing Cloud Service with any hardware or software not supplied by Oracle or not identified by Oracle in the applicable program documentation as compatible with the Oracle Eloqua Marketing Cloud Service; and

(ii) any problems caused by any modification to any version of the Oracle Eloqua Marketing Cloud Service not made by Oracle or not identified by Oracle in the applicable program documentation writing.

5.1.4 Oracle Cloud Support

The following additional support services apply to the Oracle Eloqua Marketing Cloud Services:

- Non-technical Customer service assistance is provided during Oracle business hours (8:00 to 20:00) local time, based on Customer's primary address stated in the ordering documents for the services.

5.2.2 Live Telephone Support

Customer's technical contacts and end user contacts may access live telephone support for the Oracle Eloqua Marketing Cloud Services via the phone numbers and contact information found at http://www.oracle.com/us/corporate/acquisitions/eloqua/support-1926306.html.

Appendix B – Oracle Responsys Marketing Platform Cloud Service

This appendix applies to the additional feature of the Oracle Responsys Marketing Platform Cloud Service, excluding Responsys Automatic Failover for Transactional Messages Cloud Service, and sets forth modifications to the Oracle Cloud Hosting and Delivery Policies for such Cloud Service, as follows:

1.2 Network Access Control

This section is not applicable.

Appendix C – Oracle Standalone Cobrowse Cloud Service and Oracle RightNow Cobrowse Cloud Service

This appendix applies to the Oracle Standalone Cobrowse Cloud Service and the Oracle RightNow Cobrowse Cloud Service, and sets forth modifications to the Oracle Cloud Hosting and Delivery Policies for such Cloud Services, as follows:

Access
Oracle may access your services environment to perform the Cloud Services including the provision of service support.

1.1 User Encryption for External Connections
This section is not applicable.

1.2 Network Access Control
This section does not apply to grid servers used for the Cloud Services.

1.4 Anti-Virus Controls
This section is not applicable.

1.5 Firewalls
This section does not apply to grid servers used for the Cloud Services.

1.11 Data Management / Protection
This section is not applicable.

1.11.1 Physical Media in Transit
This section is not applicable.

1.11.2 Data Disposal
This section is not applicable.

1.11.4 Data Privacy
This section is not applicable.

1.12 Regulatory Compliance
This section is not applicable.

3.5.1 Customer Monitoring & Testing Tools
This section is not applicable.

3.5.3 Automated Workloads
This section is not applicable.

4. Oracle Cloud Change Management Policy
The Oracle Cloud Change Management Policy (Section 4) is not applicable.

6. Oracle Cloud Suspension and Termination Policy
The Oracle Cloud Suspension and Termination Policy (Section 6) is not applicable.

Appendix D – Oracle Marketing Cloud Service (Formerly Known as Bluekai)

This appendix applies to the Oracle Marketing Cloud Service (formerly known as Bluekai) and sets forth modifications to the Oracle Cloud Hosting and Delivery Policies (the "Delivery Policies") for such Cloud Service. Unless otherwise specified herein, each section set forth below shall apply in lieu of the original corresponding section in the Delivery Policies:

Access
Oracle may access your services environment to perform the Cloud Services including the provision of service support.

1.1 User Encryption for External Connections

Customer access to the system is through the Internet. SSL encryption technology is available for Oracle Cloud Service access. 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. SSL is implemented or configurable for all web-based SSL 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. In some cases, a third-party site used with cloud services and not under the control of Oracle may force a non-encrypted connection. In some cases, a third party site (such as Facebook) that Customer wishes to integrate with the Cloud Service may not accept an encrypted connection. For 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.

1.4 Anti-Virus Controls

Oracle Cloud employs industry standard anti-virus software. 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.

1.7 Physical Security Safeguards

Oracle provides secured facilities for office locations infrastructure, including:

- 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 co-locations and cloud provider sites, which currently include safeguards which are compliant with SOC2 and/or SOC 1 standards, which include appropriate physical security programs.

1.8 System Access Control & Password Management

Access to Cloud systems is controlled by restricting access to only authorized personnel. Oracle enforces password policies on 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 service; although Customer does not have direct account management access, Customer must instruct Oracle in writing on any desired administrative configuration set-ups and changes.

1.9 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; although Customer does not have direct account management access, Customer must instruct Oracle in writing on any desired administrative configuration set-ups and changes.

1.10 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 makes generally available for designated Oracle customer-facing portals or interfaces, 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.

1.11.1 Physical Media in Transit

This section is not applicable.

1.11.4 Data Privacy

This section is not applicable.

1.12 Regulatory Compliance

Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud Service. Customer must make Oracle aware of any technical requirements that result from its regulatory obligations prior to contract signing. Customer must not provide Oracle with personal information, including without limitation health, payment card or other sensitive personal information.

2.1 Oracle Cloud Services Backup Strategy

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. Oracle typically does not update, insert, delete or restore Customer data on behalf of Customer. However, on an exception basis and subject to written approval and additional fees, Oracle may assist Customer to restore data from backups.

3.2 Target System Availability Level of Oracle Cloud Service

Oracle works to meet the following Target System Availability levels, for the measurement period of one calendar month, commencing at Oracle's activation of the Customer's Services Environment of the production environment:

Applicable System	**Target System Availability**
Production Service	99.5%
Tag and Pixel Serving Operations	99.9%

3.3 Definition of Availability and Unplanned Downtime

The 2nd bullet, below, is removed from the list:

- Planned outages, scheduled and 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;

4.1.2 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. Each such change event is considered planned 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 either the core system maintenance or the program upgrade window. Oracle will work to provide up to 60 days prior notice of the anticipated unavailability.

6.1 Termination of Cloud Services

Sections 6.1.2, 6.1.3, and 6.1.4 are not applicable.

6.1.1 Termination of Cloud Services

For a period of up to 121 days after the termination or expiration of production services under the ordering document, Oracle will make available Customer production data for the purpose of retrieval by Customer. Oracle has no obligation to retain the data for Customer purposes after this 121 day post termination period. Oracle Customer Support Identifiers (CSIs) are terminated at the end of the 121 day period.