Oracle Cloud Enterprise Hosting and Delivery Policies
Effective Date: Dec 1, 2015
Version 1.6

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.

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
6. Oracle Cloud Support Policy
7. 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. TLS encryption technology is available for Oracle Cloud Service access. TLS 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. TLS is implemented or configurable for all web-based TLS certified programs 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 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 Segregation in Networks
Oracle's data centers contain isolated networks used to deliver Cloud Services to Oracle Cloud Customers. Networking technologies are deployed in a layered approach designed to protect Customer data at the physical, data link, network, transport, and program level. Access controls are multi-tiered, consisting of the network, system, database, and program layers. Access is based on a "deny by default" policy.

1.3 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. The dedicated network functions as a secure access gateway between support systems and target program and database servers. Regional gateways are synchronized forming a meshed global array designed to provide continuity of support operations in the event any one of the gateways were to fail. 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. Cryptographic controls are implemented to provide Cloud operations and support with secured, easily configured access to target programs.

1.4 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 work to address internal issues that may impact availability.

1.5 Network Routing Control

1.5.1 Routers
Router controls implemented for Oracle Cloud provide the connection point between the Oracle Cloud Services and the Internet Service Provider(s). Border routers are deployed in a redundant, fault tolerant configuration. Routers are also used to enforce traffic policies at the perimeter.

1.5.2 Firewalls
Oracle Cloud Services utilize firewalls to control access between the Internet and Oracle Cloud by allowing only authorized traffic. 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, to identify authorized sources, destinations, and traffic types.

1.6 Network Security Management

1.6.1 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.

1.6.2 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.

1.6.3 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.

1.6.4 Anti-Virus Controls
Oracle Cloud employs anti-virus software to scan uploaded files when deemed necessary by Oracle. Virus definitions are updated daily.

1.6.5 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.

1.7 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.

1.8 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

1.9 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.

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 Customer’s End User accounts. Customer may configure the programs and additional built-in security features.

1.10 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.

1.11 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.

1.12 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 subscribed Oracle Cloud service.

1.12.1 Data Protection
Oracle Cloud offers several standard encryption technologies and options to protect data, depending on the particular Cloud Service, while in transit or at rest. For network transmission, Customers may choose to use secured protocols (such as TLS) to protect their data in transit over public networks. Secured protocols available in the Oracle Cloud offer strong encryption algorithms.

Strong key management policies and processes are employed for any Oracle Cloud encryption.

1.12.2 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.

1.12.3 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.

1.12.4 Secure File Transfer
Secure file transfer functionality is built on commonly used network access storage platforms and uses secured protocols for transfer (such as SFTP). The functionality can be used to upload files to a secured location, most commonly for data import/export on the Oracle Cloud hosted service, or downloading files at service termination.

1.12.5 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 and, depending on the nature of the activity, GIS defines escalation paths and response teams to address those incidents. GIS will work with Customer, and 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 report such misappropriation to Customer within 72 hours of making such determination, unless prohibited by law.

1.12.6 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 personal data that resides on Oracle systems to which Oracle may be provided access in connection with the provision of Cloud Services. The Data Processing
Agreement 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:

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

### 1.13 Regulatory Compliance

Oracle Cloud Services operate under Policies which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected, as described by ISO/IEC 27001.

The Information Security Management System Family of Standards (ISO/IEC 270xx) are published by ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission), and are a comprehensive reference for information security management, data protection and risk management for organizations of all types and sizes.

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 audited to PCI DSS or FISMA/NIST standards and additional certifications and attestations to specific regulatory frameworks for 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.

### 1.14 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](http://www.oracle.com/us/support/assurance/overview/index.html).
2. Oracle Cloud System Resiliency Policy

The resiliency and backups described in this Policy apply only for Oracle Cloud services. Customer is solely responsible for developing a business continuity plan to ensure continuity of its own operations in the event of a disaster and for backing up and recovering any non-Oracle software.

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 Program Servers

Customer’s environment consists of a set of one or more physical servers or virtual servers that provide services to Customer. The overall program tier functionality may be distributed across multiple physical servers or virtual servers.

2.5 Redundant Database Servers

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

2.6 Redundant Storage

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

2.7 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. 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 Disaster Recovery Service Policy

3.1 Scope

This Policy applies only to Customer’s production environments within Oracle Cloud Services. The activities described in this Policy do not apply to Customer’s own disaster recovery, business continuity or backup plans or activities, and Customer is responsible for archiving and recovering any non-Oracle software.

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 Customer production 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. Customer’s production standby (secondary site) environment will reside in a data center separate from Customer’s 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. For a major regional jurisdictional area (e.g., the United States or the European Union), Oracle operates both a production and secondary site within that region.

Customer data is replicated in physically separate facilities in order to restore full services in the event of a disaster at a primary site. Backups are for Oracle’s sole use in the event of a disaster.

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.

Note: the RTO and RPO described below do not apply to Customer customizations that depend on external components or third-party software. During an active failover event, non-critical fixes and enhancement requests are not supported. Customer will be solely responsible for issues arising from third party software and customizations (CEMLIs) to Oracle programs and services.

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.

3.3.2 Recovery Point Objective
Recovery point objective (RPO) is Oracle’s objective for the maximum possible length of time during which data could be lost, in the event of a disaster. The RPO is 1 hour from the occurrence of a disaster, excluding any data loads that may be underway when the disaster occurs.
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 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 Customer’s user work stations as set forth in the Cloud Services Program Documentation, Oracle works to meet the Target Service Availability Level in accordance with the terms set forth in this Policy.

4.2 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.
4.3 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, 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.

4.4 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.

4.4.1 Reporting of Availability

Oracle will provide Customer with access to a Customer notifications portal. This portal will provide metrics on the System Availability Level for Cloud Services purchased under the ordering document. For those Cloud Services for which such metrics are not available via the Customer notifications portal, Oracle will provide metrics on the System Availability Level upon receipt of a Service Request submitted by Customer to Oracle requesting the metrics.

4.5 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.
4.5.1 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.

4.5.2 Customer Monitoring & Testing Tools
Due to potential adverse impact on service performance and availability, Customer may not use their 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.

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

4.5.4 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 annually. Oracle may require that a written statement of work be executed to perform such testing and validation work.

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, upgrades and updates, and Customer specific changes. 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. The typical scheduled maintenance period is once a month on Friday, initiating at approximately 20:00 data center local time, lasting around 10 hours. There are exceptions to this schedule for some Cloud services; further documentation is available on My Oracle Support in Knowledge Article 1681146.1: https://support.oracle.com/epmos/faces/DocumentDisplay?id=1681146.1.

Oracle will work to provide prior notice of modifications to the standard maintenance period schedule. 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.

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.

5.1.3 Data Center Migrations
Oracle may migrate Customer services between production data centers in the same data center region in order to recover Customer services or in the case of disaster recovery. For all other data center migrations, Oracle will provide a minimum of 30 days notice to Customer.

5.2 Software Versioning

5.2.1 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). 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, the Disaster Recovery 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.

5.2.2 End of Life
Oracle will not support older versions beyond the End of Life Policy described as follows. Oracle will host and support only the designated GA versions of an Oracle Cloud Service. All other versions of the service are considered as “end of life” (EOL). Oracle does not provide Cloud Services for EOL versions. Customers are required to complete the services upgrade to the latest version before the EOL of a given version. Customer acknowledges that failure to complete the upgrade prior to the EOL of a Cloud Service version may result in an upgrade automatically performed by Oracle or a suspension of the services. 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.

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.

6. 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.
6.1 Oracle Cloud Support Terms

6.1.1 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.

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

6.1.3 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 service training 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.

6.1.4 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.

6.2 Oracle Cloud Customer Support Systems

6.2.1 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.

6.2.2 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.
6.3 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 6.2 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.

6.4 Change to Service Request Severity Level

6.4.1 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.

6.4.2 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.

6.4.3 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.

6.4.4 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.

6.5 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.

6.6 Policy Exceptions
Customer questions or requests for an exception to the Oracle Cloud Hosting and Delivery Policy must be made via a service request with the Cloud Customer Support Portal applicable to the service (e.g., My Oracle Support).

7. Oracle Cloud Suspension and Termination Policy

7.1 Termination of Cloud Services

7.1.1 Termination of Cloud Services
Upon termination or expiration of services under the ordering document, or at Customer’s request, Oracle will delete or otherwise render inaccessible the production environments and 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.

For a period of up to 60 days after the termination or expiration of 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, and Oracle shall remove or render inaccessible Customer data within the service.

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

7.1.3 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).

7.1.4 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.

7.2 Suspension Due to Violation
If Oracle detects a violation of, 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.
7.3 Exportable Data
The following Customer data is exportable by Oracle from the Cloud Services production environment at termination.

- Database Data: All transactional data.
- Document Attachments: All document attachments that were uploaded by Customer or attached to a business transaction or workflow.
Appendix A – Oracle Responsys Marketing Platform Cloud Service

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

1.2 Segregation in Networks
This section is not applicable.

3.3.1 Recovery Time Objective
The last sentence of this section is modified to read as follows: “The RTO for the Oracle Responsys Automatic Failover for Transactional Messages Cloud Service is 30 minutes from the declaration of a disaster.”

3.3.2 Recovery Point Objective
The last sentence of this section is modified to read as follows: “The RPO for the Oracle Responsys Automatic Failover for Transactional Messages Cloud Service is 15 minutes from the occurrence of a disaster.”

4.2 Target System Availability Level of Oracle Cloud Service
Oracle works to meet a Target System Availability Level of 99.9% of the production Oracle Responsys Automatic Failover for Transactional Messages Cloud Service, for the measurement period of one calendar month, commencing at Oracle’s activation of the production environment.
Appendix B – Oracle Field Service Cloud Service

This appendix applies to the Oracle Field Service Cloud Service, and sets forth modifications to the Oracle Cloud Enterprise Hosting and 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:

Part 1 – Modifications for ETAdirect Enterprise and ETAdirect Professional

1.1 User Encryption for External Connections
Customer access to the system is through the Internet. TLS encryption technology is available for Oracle Cloud Service access. TLS 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. TLS is implemented or configurable for all web-based TLS certified programs 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 the Oracle Field Service Cloud Service will be provided to Customer upon request. 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.

1.12.2 Physical Media in Transit
This section is not applicable.

3.3.1 Recovery Time Objective
The last sentence of this section is modified to read as follows: “The RTO for ETAdirect Professional is 5 hours from the declaration of a disaster. The RTO for ETAdirect Enterprise is 4 hours from the declaration of a disaster.”

5.1.3 Data Center Migrations
This section is not applicable.

Part 2 – Modifications for ETAworkforce

Access
This section is not applicable.

Hours of Operation
This section is not applicable.

1. Oracle Cloud Security Policy
This section is not applicable.

2. Oracle Cloud System Resiliency Policy
This section is not applicable.

3. Oracle Cloud Disaster Recovery Service Policy
This section is not applicable.

4. Oracle Cloud Service Level Objective Policy
This section is not applicable.
5. **Oracle Cloud Change Management Policy**
   This section is not applicable.

6. **Oracle Cloud Support Policy**
   Below paragraph is added to the end of the section:

   Oracle has no obligation of any kind to provide support services for problems in the operation or performance of ETAworkforce caused by any of the following: (i) non Oracle software or hardware products or carrier network and setup issues; (ii) alteration, damage, or modification (including but not limited to configuration changes) to the delivered software not made by or expressly authorized by Oracle; (iii) problems caused by Your negligence, abuse or misapplication, or (iv) Your use of the software other than as permitted by law or as provided in the relevant documentation. Oracle reserves the right to suspend and/or disconnect services if any of the foregoing are deemed a threat to Oracle’s systems or Cloud Services.

7.1 **Termination of Cloud Services**
   This section is not applicable.

7.3 **Exportable Data**
   This section is not applicable.