ORACLE

Oracle NetSuite Hosting & Support Delivery Policies

Effective Date: 19-January-2024

Table of Contents

OVERVIEW

These Oracle NetSuite Hosting and Support Delivery Policies (these "**Hosting Policies**") describe the Cloud Service as defined in the Agreement (defined below), which include only the following (each a "Cloud Service" and collectively, "Cloud Services"):

- NetSuite Service
- OpenAir Service
- NetSuite Connectors
- NetSuite CPQ

These Hosting Policies may reference other Oracle Cloud policy documents. Any reference to "You" in these Hosting Policies or in such other policy documents shall be deemed to refer to "Customer" as defined in Customer's Estimate/Order Form ("**Order**") or the Agreement. For purposes of these Hosting Policies, (1) "Agreement" means the applicable agreement referenced in Customer's Order that governs Customer's use of the Cloud Service and which references these policies. Additionally, the following also applies to these Hosting Policies:

- References in these Hosting Policies to the following terms shall have the same meaning as set forth in the Subscription Services Agreement for NetSuite Connectors: (a) "Customer" shall include "Subscriber", (b) "Customer Data" shall include "Subscriber Data", and (c) "Term" shall include "Initial Term" and any "Renewal Term".
- References in these Hosting Policies to "Services Period" shall mean the term of the Cloud Services Customer has purchased as specified in Customer's Order (for example, 12 months).

Capitalized terms that are not otherwise defined in these Hosting Policies shall have the meaning ascribed to them in the Agreement (including documents incorporated into the Agreement) or Customer's Order, as applicable.

Customer's Order or Agreement may include additional details or exceptions related to specific Cloud Services. The Cloud Services are provided under the terms of the applicable Agreement and Customer's Order. Oracle's delivery of the Cloud Services is conditioned on Customer's and Customer's Users' compliance with Customer's obligations and responsibilities defined in such documents and incorporated policies. These Hosting 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, functionality, security, or availability of the Cloud Services provided during the Services Period of Customer's Order.

These Hosting Policies do not apply to any Third Party Applications (as defined in the Agreement), any services sold by Oracle which are subject to separate terms and conditions (other than the Agreement), including but not limited to NetSuite US Payroll Service, or as otherwise specified in Customer's Order (including in the applicable item descriptions or Service Descriptions). Additional exceptions to these Hosting Policies are outlined within each applicable section.

DEFINITIONS

"Advanced Customer Support" is a managed service which Oracle offers on a subscription basis. Advanced Customer Support is provided by Oracle to assist customers in their use of the Cloud Service or specific components of the Cloud Service.

"**Alternative Solution**" means a solution or correction to an Incident that allows the Cloud Service to function substantially in accordance with the User Guides.

"**Authorized Contacts**" means the named Customer employees or authorized agents who: (i) have sufficient technical expertise, training and/or experience with the Cloud Service to perform the Customer's obligations as outlined herein; (ii) are responsible for all communications with Oracle regarding the Oracle NetSuite Support Services described in Section II of these Hosting Policies, including case submission and Incident reports; and (iii) who are authorized by Customer to request and receive Support Services for the Cloud Service on behalf of the Customer.

"**Basic Support**" is Oracle's basic Support Services described herein, which is included in a current subscription to the Cloud Service. In addition, Basic Support expands the coverage for Severity 1 issues to 24x7.

"**Business Days**" are Monday to Friday during Normal Business Hours, excluding Oracle company holidays.

"**Enhancement Request**" means a request by Customer to add functionality or enhance performance beyond the specifications of the Cloud Service and are not included as part of Support Services.

"**First Level Support**" means any support relating to calls from Customer's customers, end users or affiliates or general resolution of user errors, network errors, provisioning errors or Internet delays or malfunctions.

"**Incident**" means a single support question or reproducible failure of the Cloud Service to substantially conform to the functions and/or specifications as described in User Guides and reported by an Authorized Contact.

"**Normal Business Hours**" are 8:00 a.m. to 6:00 p.m. on Business Days in the time zone of the address for the Customer's headquarters listed on the Agreement.

"**Premium Support**" means Oracle's enhanced level of Support Services. In addition to the Basic Support Services described herein, if Customer is entitled to Premium Support, the Normal Business Hours for Severity 1 and Severity 2 issues will be expanded to 24x7 coverage with improved Response Time Goals and additional Authorized Contacts are provided.

"Primary DC" shall mean the primary data center in which Customer Data is stored.

"**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information ("PII")" or the equivalent term under Applicable Data Protection Law.

"Safeguards" shall mean physical and technical safeguards.

"Security Incidents" shall mean an actual unauthorized disclosure, or reasonable belief that there has been an unauthorized disclosure, by Oracle of Customer Data containing unencrypted information to any unauthorized person or entity.

"**SuiteAnswers**" is the online support portal that is accessible 24x7.

"**Support Services**" means Basic Support and optional Premium Support services for the Cloud Service provided by Oracle under the terms set forth herein and as further defined in the Agreement, but does not include First Level Support or Enhancement Requests. Customer's level of Support Services shall be determined by the level of Support Services that such Customer has procured. Support Services are provided in English but may be provided in other languages if and when available at Oracle's sole discretion.

I. ORACLE NETSUITE CLOUD SERVICES DATA SECURITY POLICIES

For the Cloud Service procured on the applicable Order, Oracle shall maintain commercially reasonable administrative Safeguards designed for the protection, confidentiality, and integrity of Customer Data. All such Safeguards shall be commensurate with the importance of the Customer Data being protected, but in no event less protective than safeguards that Oracle uses to protect its own information or data of similar importance, or as required by applicable law.

The Safeguards described herein are applicable during the Services Period of Customer's Order; however, Safeguards described in these Hosting Policies are not comprehensive and such Safeguards may change during the Services Period of the applicable Order as applicable third party security audits, compliance standards and/or certifications evolve/change over time, provided that any such changes to Safeguards will not materially decrease the overall security of the Cloud Service during the Services Period of the applicable Order.

During the Services Period, Oracle shall comply with all obligations regarding Customer Data, including, without limitation, Oracle's obligations to maintain commercially reasonable Safeguards as provided herein.

A. Oracle NetSuite Security Policy

Oracle has, and will maintain, a security policy for its security organization that requires security training and privacy training as part of the training package for Oracle security personnel supporting the Cloud Service.

B. Oracle NetSuite Security Organization

Oracle has, and will continue to have, a dedicated security organization that is responsible for the ongoing monitoring of Oracle's security infrastructure, the review of Oracle products and services, and for responding to security incidents.

C. Data Storage and Handling

Storage medium or any equipment with storage capability, including mobile media, used to store Customer Data will be secured and hardened in accordance with industry standard practices, such as:

i. Oracle will maintain a reasonable asset management policy to manage the life cycle (commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of such media;

ii. Decommissioned media containing Customer Data will be destroyed in accordance with NIST 800-88 at the Moderate level of sensitivity (or similar data destruction standard);

iii. Customer Data will be logically segmented from Oracle data and other Oracle customers' data; and

iv. Database fields in the Cloud Service designated for credit card data information and social security numbers will be encrypted, and Oracle will not process such Customer Data in test, development, or non-production environments.

D. Data Transmission

Customer's access to the Cloud Service is through a secure communication protocol specified by Oracle. Oracle will use strong cryptography and security protocols consistent with industry standards, as documented in the User Guides for the Cloud Service.

E. Incident Reponse

Oracle will monitor a variety of communication channels for known incidents, and Oracle's security team will react promptly to such known incidents. In the event of a Security Incident, Oracle will: (i) notify Customer in accordance with Oracle's obligations under applicable law or regulatory requirement, to the extent an applicable security breach law applies to such Security Incident; and (ii) perform a penetration test after corrective actions are implemented, if applicable, with a test results summary to be provided to Customer, and such test results to be deemed Oracle Confidential Information.

Incidents involving Personal Information shall be managed according to the provisions set forth within the Oracle Data Processing Agreement.

F. Change Management

Oracle maintains a change management policy to ensure changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.

G. Server Operating Systems

Oracle servers will use a hardened operating system implementation customized for the Cloud Service. Oracle will maintain a risk-based prioritized patch management policy.

H. Access Control and Privilige Management

Oracle employs systems and processes to limit physical and logical access based on least privileges and segregation of duties to ensure critical data can only be accessed by authorized Oracle personnel.

I. User Accounts

Customer will have control over the creation, deletion, and suspension of User roles within the Cloud Service, as documented in the applicable Cloud Service User Guides. The Cloud Service allows Customer to perform administrative functions.

J. Oracle Responsibilities and Policy Controls

Oracle will implement measures to ensure Customer Data is processed only in accordance with the terms and conditions of the Agreement.

K. Password Configuration

As documented in the applicable Cloud Service User Guides, certain Cloud Services allow Customer to apply its own password and authentication policies via the Cloud Service's configurable policy settings and when using the single sign on functionality in the Cloud Service.

L. Network Connectivity Security Requirements

Oracle will protect its infrastructure with multiple levels of secure network devices. All remote access to the Cloud Service environments by Oracle personnel that have access to Customer Data must be through one or a combination of the following: virtual private network, multi-factor authentication, mutual authentication, client trust scoring, or other authentication methods with an equal or higher level of security.

M. Audits and Certifications

The following security audits and certifications are relevant to the Cloud Service, as set forth below:

i. PCI-DSS. Payment Card Industry Data Security Standard ("PCI DSS") is a worldwide information security standard for organizations that handle branded credit cards such as Visa, Master Card, American Express, etc. The PCI standards are mandated by the card brands and run by the Payment Card Industry Security Standards Council. During the Services Period of the applicable Order, Oracle shall maintain PCI DSS compliance for those portions of the Cloud Service that are designated by Oracle as being designed to store and process credit card data.

Customer is responsible for ensuring that its use of the Cloud Service to store or process credit card data complies with applicable PCI DSS requirements and shall not store credit card and social security data in the Cloud Service except in the designated encrypted fields for such data. Any changes made to the Cloud Service by or on behalf of Customer may affect Customer's compliance with PCI DSS requirements and Customer shall be solely responsible for ensuring that any such changes are compliant with PCI DSS requirements.

ii. SOC Report Attestations. The American Institute of CPAs ("AICPA") has established System and Organization Controls ("SOC") frameworks for evaluating and reporting on the effectiveness of a service organization's controls that address specific user needs. With respect to the Cloud Service, Oracle shall ensure performance of annual third-party attestation reports completed in accordance with the AICPA and IFAC Standards for Assurance Engagements:

a. Oracle shall ensure performance of an annual SOC 1 / ISAE 3402 Type II report.

b. Oracle shall ensure performance of an annual SOC 2 Type II report, for the Security, Availability, and Confidentiality attributes.

c. Any material findings that lead to a qualified opinion on the SOC reports will be promptly addressed with the development and implementation of a corrective action plan by Oracle's management.

iii. ISO 27001. ISO 27001 is a leading international standard published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") for measuring information security management systems ("ISMS"). This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS.

Oracle shall ensure performance of a third-party certification audit of Oracle's ISMS against the requirements of the ISO 27001 standard.

iv. Customer may submit a request for a copy of Oracle's final: a) SOC 1 / ISAE 3402 Type II report; b) SOC 2 Type II report; and (c) ISO 27001 certificate and Statement of Applicability ("SOA"). Any such reports, certificates and supporting documentation provided by Oracle in connection with this Section I.M.iv are deemed Oracle Confidential Information.

v. If similar third-party audits, standards and/or certifications become available in the future, Oracle may choose to perform such audit and/or certify to such established industry standard selected by Oracle in place of those in this Section I.M.

N. Data Center Environments and Physical Security

The following is a general description of Oracle's various data center environments and efforts to ensure physical security in these environments.

Data centers running Cloud Services in Oracle Cloud Infrastructure ("**OCI**") are governed by Section 1.2, "Physical Security Safeguards", and Section 2.1, "Oracle Cloud Services High Availability Strategy", of the ***Oracle Cloud Hosting and Delivery Policies*** which are found at www.oracle.com/contracts/cloud-services or other URL as designated by Oracle.

O. Disaster Recovery

Oracle maintains an internal Disaster Recovery plan ("**Internal DR Plan**") intended to provide service restoration capability of Customer's production accounts in the event of a disaster, as declared by Oracle in its sole discretion. If Oracle determines that an event constitutes a disaster requiring execution of its Internal DR Plan, Oracle will work to restore the production environments of the affected Cloud Service.

Recovery Time Objective: Recovery Time Objective ("**RTO**") is Oracle's objective for the maximum period of time between Oracle's decision to activate the processes described herein and the point at which Customer can resume production operations in an alternative site. If the decision to activate disaster recovery processes is made during the period in which an upgrade is in process, the disaster recovery process is initiated and completed first, followed by completion of the upgrade.

Recovery Point Objective: Recovery Point Objective ("**RPO"**) is Oracle's objective for the maximum period of data loss measured as the time from which the first transaction is lost until the time the disaster occurs (as recognized by Oracle). The RPO does not apply to any data loads that are underway when the disaster occurs.

For the following Cloud Service, the RTO is 12 hours and the RPO is 1 hour.

- NetSuite Service

If the NetSuite Service fails to achieve the RTO, Customer will be entitled, as its sole and exclusive remedy, to a service credit for use of the Cloud Service in accordance with the terms set forth in Section III. (Oracle NetSuite Service Level Commitment).

Customer may experience some delays in the operation of the Cloud Service for the duration of the disaster event.

During active failover events or recovery operations, Oracle's delivery of non-critical bug fixes and enhancement requests are suspended.

P. Risk Assessments

Oracle shall perform a risk assessment of the Cloud Service every year. This assessment shall include an evaluation of risks to the confidentiality, integrity, and availability of Customer Data which resides on the Cloud Service and a documented plan to correct or mitigate those risks in its security policy to an acceptable residual-risk level as determined by Oracle, in its sole discretion.

Q. Handling of Personal Information

Oracle will process Personal Information as part of the provision of its Services in accordance with the applicable Agreement and will be responsible for the compliance of its respective obligations under the applicable data protection laws. In handling and processing of Personal Information, Oracle shall implement and maintain appropriate technical and organizational security measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

R. Use of Services

The Cloud Service may not be delivered to, or accessed by, Users in Venezuela, nor may the Cloud Service or any output from the Services be used for the benefit of any individuals or entities in Venezuela including, without limitation, the Government of Venezuela.

S. SECTION I EXCEPTIONS & EXCLUSIONS

- Section I.M.i. (Audits and Certifications, PCI-DSS) does not apply to Open Air Service.
- Section I.M (Audits and Certifications) does not apply to:
    - NetSuite QuickStart Edition Early Adopter (formerly called: NetSuite New Starter Edition)
    - NetSuite Connector Cloud Service
    - NetSuite CPQ Cloud Service
- Section I.O (Disaster Recovery) does not apply to:
    - NetSuite Connector Cloud Service
    - NetSuite Point-of-Sale (POS) Cloud Service
    - NetSuite CPQ Cloud Service
    - Open Air Service
    - NetSuite QuickStart Edition Early Adopter (formerly called: NetSuite New Starter Edition)
    - Non-production environment(s), including without limitation, sandbox accounts, development accounts, demo accounts, and trial accounts
    - RTO does not apply to any NetSuite Suite Commerce Cloud Services (Note: Oracle will begin the recovery process within 12 hours, but final service readiness depends on the customer's store configuration (specifically, item volume and complexity) which may exceed the 12-hour RTO).

II. ORACLE NETSUITE SUPPORT SERVICES

A. General

Subject to Customer's procurement of Support Services (defined herein), the terms of this Section II (the "**Support Terms**") describe Oracle's provision of Support Services to Customer pursuant to the terms of the Agreement and these terms in accordance with the level of Support Services that Customer has procured.

B. Scope of Support Services

i. Subject to these Support Terms, Oracle shall address all Incidents which may arise from Customer's use of the Cloud Service in accordance with Sections II.D (Incident Reporting and Response Times) and II.E (Exclusions and Exceptions from Support Services below.

ii. Oracle shall not have any obligation to provide Support Services with respect to any:

   a. adaptations, configurations or modifications of the Cloud Service made by the Customer or any third party, including those that are made using SuiteScript or JavaScript;

   b. First Level Support, which shall be provided by Customer;

   c. Enhancement Requests; or

   d. any items excluded pursuant to Section II.E (Exclusions and Exceptions from Support Services).

iii. Oracle may offer Professional Services or Advanced Customer Support to help resolve issues that fall outside the scope of the Support Services. Any engagement of Professional Services or Advanced Customer Support shall be provided under a separate agreement and/or Order and shall be subject to the Agreement and Oracle's then-current consulting fees and terms.

C. Termination

Notwithstanding anything to the contrary herein or in the applicable Agreement, these Support Terms shall terminate upon expiration or termination of the Agreement or expiration or termination of Customer's right to access the applicable Cloud Service.

D. Incident Reporting and Response Times

i. Authorized Contacts. All reports of Incidents must be made to Oracle by the Authorized Contact(s). The primary method for a Customer to report an Incident is via SuiteAnswers. The foregoing notwithstanding, Customers procuring Basic Support may notify Oracle of S1 (defined in Section II.D.iii (Severity Levels)) incidents via telephone if Customer's access to SuiteAnswers is unavailable. Customers procuring Premium Support may notify Oracle of S1 and S2 (defined in Section II.D.iii (Severity Levels)) Incidents via telephone if Customer's access to SuiteAnswers is unavailable. Customer may substitute Authorized Contact(s) from time to time by giving Oracle prior written notice, including the relevant contact information for any new Authorized Contact.

   Permitted number of qualified Authorized Contacts

   - Basic Support: 2
   - Premium Support: 4

ii. Required Information. All Incident reports must, if applicable, include the following:

   a. The Customer's identification number, provided as part of provisioning.

   b. Detailed instructions that allow Oracle to reproduce the specific usage that caused the Incident being reported.

   c. Exact wording of all related error messages.

   d. A full description of the Incident and expected results.

   e. Any special circumstances surrounding the discovery of the Incident.

   f. For S1 Incidents, provide an additional point of contact.

Oracle may share such information and other information about Incidents with its contractors, vendors and/or third party application providers to support Oracle's provision of the Support Services described herein.

iii. Severity Levels. Oracle will work with Customer and will assign the appropriate severity level to all Incidents according to the definitions below (each individually a "**Severity Level**"). Severity Levels are assigned to allow prioritization of incoming Incidents. Oracle may reclassify Incidents based on the current impact on the Cloud Service and business operations as described below. In the event Oracle determines that an Incident is in fact an Enhancement Request, it shall not be addressed under these Support Terms. Severity Levels are defined as:

a. "**Severity Level 1**" or "**S1 (Critical)**" means an Incident where Customer's production use of the Cloud Service is stopped or so severely impacted that the Customer cannot reasonably continue business operations. It may result in a material and immediate interruption of Customer's business operation that will cause a loss of Customer data and/or restrict availability to such data and/or cause significant financial impact.

b. "**Severity Level 2**" or "**S2 (Significant)**" means an Incident where one or more important functions of the Cloud Service are unavailable with no acceptable Alternative Solution. Customer's implementation or production use of the Cloud Service is continuing but not stopped; however, there is a serious impact on the Customer's business operations.

c. "**Severity Level 3**" or "**S3 (Less Significant)**" means an Incident where: (a) important Cloud Service features are unavailable but an Alternative Solution is available, or (b) less significant Cloud Service features are unavailable with no reasonable Alternative Solution; Customers experience a minor loss of business operation functionality and/or an impact on implementation resources, or (c) Customer poses questions regarding basic functionality of the Cloud Service. This category is only available to Customers purchasing Premium Support.

d. "**Severity Level 4**" or "**S4 (Minimal)**" means an Incident that has a minimal impact on business operations or basic functionality of the Cloud Service. This category is only available to Customers purchasing Premium Support.

iv. Oracle's Obligations. Oracle will make available Support Services access during Normal Business Hours for the Customer to report Incidents and receive assistance. On receipt of an Incident report, Oracle shall establish whether there is an Incident for which the Customer is entitled to Support Services under these Support Terms and, if so, shall:

a. Confirm receipt of the Incident report and notify Customer of the Incident case number that both parties must then use in any communications about the Incident.

b. Work with Customer to set a Severity Level for the Incident based on the criteria set forth herein.

c. Analyze the Incident and verify the existence of the problem.

d. Give the Customer direction and assistance in resolving the Incident pursuant to the terms described herein.

v. Response Time Goals.

	Severity Level 1	Severity Level 2	Severity Level 3	Severity Level 4
Basic Support	2 hours	Not Applicable[1]	Not Applicable[2]	Not Applicable

Premium Support	1 hour	2 hours	8 hours	2 Business Days

[1] ***Note**: for customers who purchased support prior to Dec 1, 2019, S2 response time is 4 hours.*
[2] ***Note**: for customers who purchased support prior to Dec 1, 2019, S3 response time is 2 Business Days.*

vi. Customer Obligations.

a. Oracle's obligation to provide Support Services under these Support Terms is conditioned upon Customer:

1. paying all applicable fees for Support Services prior to the date the Incident is reported;
2. having valid access to the Cloud Service;
3. providing Oracle with all reasonable assistance and providing Oracle with data, information and materials as that are reasonably necessary;
4. procuring, installing and maintaining all equipment, telephone lines, communication interfaces and other hardware and software necessary to access the Cloud Service;
5. providing all First Level Support;
6. providing appropriate contact information for all Authorized Contacts(s);
7. utilizing SuiteAnswers knowledge base for self-help research of known solutions, and
8. utilizing SuiteAnswers incident reporting portal to log all incident cases, except for Basic Support customers who are permitted to log S1 incidents and Premium Support customers who are permitted to log S1 and S2 incidents via telephone as set forth in Section II.D.i (Authorized Contacts).

b. For the duration of the initial term and any renewal term(s) during which Customer has purchased Support Services, Customer shall purchase and maintain the same level of Support Services for all users of the Cloud Service (including without limitation any incremental licenses subsequently purchased by Customer). For clarity, Customer may not elect to purchase or renew Support Services for just a portion of its Service or of its users who can access the Service nor can Customer purchase different levels of support for a portion of its Users.

E. Exclusions and Exceptions from Support Services

Oracle will not be required to correct any Incident caused by (i) integration of any feature, program or device to the Cloud Service or any part thereof; (ii) any non-conformance caused by unauthorized misuse, alteration, modification or enhancement of the Cloud Service; or (iii) use of the Cloud Service that is not in compliance with the Agreement.

F. SECTION II EXCEPTIONS & EXCLUSIONS

Oracle will not be required to correct any Incident caused by (i) integration of any feature, program or device to the Cloud Service or any part thereof; (ii) any non-conformance caused by unauthorized misuse, alteration, modification or enhancement of the Cloud Service; or (iii) use of the Cloud Service that is not in compliance with the Agreement.

III. ORACLE NETSUITE SERVICE LEVEL COMMITMENT

A. Service Availability

Oracle commits to provide 99.7% availability with respect to the Cloud Service ordered by Customer during each calendar month of the Services Period for the applicable Order, excluding scheduled maintenance times ("**Service Availability**"). If, in any calendar month, this Service Availability is not met by Oracle, and Customer was negatively impacted (attempted to log into or access the Cloud Service and failed due to Unplanned Downtime, as defined below), Oracle shall provide, as the sole and exclusive remedy, a Service Credit based on the monthly fee for the use of the Cloud Service, as follows:

Service Availability	**<99.7% and >= 99.5%**	**<99.5% and >= 99.0%**	**< 99.0%**
Service Credit	10%	15%	25%

Oracle measures the Service Availability over each calendar month 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. "**Unplanned Downtime**" means any time during which a problem with the Cloud Service would prevent Customer from logging in or accessing the Cloud Service. Oracle shall calculate any Unplanned Downtime using Oracle's system logs and other records. Unplanned Downtime does not include any time during which the Cloud Service is not available due to any suspension or termination of the applicable Cloud Service, or any other unavailability or performance issue that results from Customer's and/or a third-party's equipment, software, services, or other technology (other than third party equipment or services within Oracle's direct control).

B. Scheduled and Unscheduled Maintenance

Scheduled maintenance does not count as Unplanned Downtime for the purposes of calculating a Service Credit as shown in the table above. Maintenance is considered to be 'scheduled' if it is communicated (i) in accordance with Section III.E (Notice), set forth below, and (ii) at least two full business days in advance of the scheduled maintenance time, although Oracle strives to communicate scheduled maintenance at least a week in advance when possible. Scheduled maintenance usually occurs outside of regular business hours for each region and generally accounts for less than 15 hours each quarter. In addition to any other scheduled maintenance Oracle may communicate, every Saturday night between 10:00pm - 10:20pm Pacific Time is reserved for scheduled maintenance as may be needed.

Oracle, in its sole discretion, may take the Cloud Service down for unscheduled maintenance, and in that event will attempt to notify Customer in advance in accordance with Section III.E. (Notice) set forth below. Unscheduled maintenance will be included in Unplanned Downtime and counted against the Service Availability set forth above.

C. Service Credit Request

In order to receive a Service Credit as described herein, Customer must email Oracle at billing@netsuite.com to request a Service Credit within 30 calendar days from the end of the month in which the Service Availability was not met, and Customer must provide details of the claim, as reasonably requested by Oracle. Any claim request which is successfully submitted will receive a response indicating the request was received. If Customer does not receive this response, the claim is deemed not received by Oracle and Customer must resubmit their claim in order for Oracle to consider the request for a Service Credit. Customers with accounts that are past due or in default to Oracle with respect to any payment or any material contractual obligations are not eligible for any Service Credit

under this Service Level Commitment. The Service Credit is valid for up to two years from the quarter for which the credit is issued.

D. Updates

This Section III of the Hosting Policies (Oracle NetSuite Service Level Commitment) may be amended at any time by Oracle in its discretion. Updates will be effective 30 days after providing notice to Customer in accordance with Section III.E. (Notice) below.

E. Notice

Notice will be provided as either: (a) a note on Customer's administrator(s)' screen presented immediately after logging into the Cloud Service, or (b) by email to the registered email address provided for the administrator(s) for Customer's account.

F. SECTION III EXCEPTIONS & EXCLUSIONS

Section III does not apply to:

- Any Sandbox, Release Preview, Beta, Education, Demo, Developer and/or debugger accounts, and any other non-production or test environments.
- NetSuite CPQ Cloud Service
- NetSuite Connectors Cloud Service

IV. ORACLE NETSUITE RESPONSE SERVICES REQUIREMENTS

A. General

Subject to the additional requirements set forth in the table below, these Response Services Requirements, which are a supplement to the Oracle NetSuite Support Services described in Section II of these Hosting Policies, shall govern the provision of specific response services described below (the "**Response Services**") and apply solely in connection with Response Services.

B. Response Services Requirements & Descriptions

	Requirements		
Response Services	**Support Services Level**	**Severity Level**	**Cloud Service**
Commerce Response Services	Premium Support	Severity Level 1 (Critical)	SuiteCommerce ("**SC**") or SuiteCommerce Advanced ("**SCA**")
Point-of-Sale Response Services	Premium Support	Severity Level 1 (Critical)	NetSuite POS module ("**NSPOS**")

"**Commerce Response Services**" or "**CRS**" means the supplemental English language Response Service for websites that were created using SC or SCA ("**Website(s)**").

"**Point-of-Sale Response Services**" or "**PRS**" means the supplemental English language Response Service for NSPOS.

Commerce Response Services. Oracle will use commercially reasonable efforts to analyze Website-related errors and help identify causation. Oracle will provide reasonable remediation assistance, help

identify a workaround, or recommend that Customer separately procure Professional Services from Oracle. Oracle may require access to Customer's sandbox and production environments of the Cloud Service ("**Customer Accounts**"). Customer agrees to provide Oracle with the level of Customer Account(s) access that is reasonably necessary for so long as Oracle requires such access and Customer shall immediately remove such access upon the completion of CRS activity.

Point-of-Sale Response Services. Oracle will use commercially reasonable efforts to analyze NSPOS-related errors and help identify causation. Oracle will provide reasonable remediation assistance, help identify a workaround, or recommend that Customer separately procure Professional Services from Oracle. Oracle may require access to Customer's sandbox and production environments of the Cloud Service ("**Customer Accounts**"). Customer agrees to provide Oracle with the level of Customer Account(s) access that is reasonably necessary for so long as Oracle requires such access and Customer shall immediately remove such access upon the completion of PRS activity.

C. Termination

The Response Service a supplemental service which is being provided at no additional cost by Oracle. Oracle may, in its sole discretion, immediately cease to provide Response Services at any time upon notice to Customer.

D. SECTION IV EXCEPTIONS AND EXCLUSIONS

The Oracle NetSuite Response Services Requirements are only available for the Cloud Services listed in the table in Section IV.B above (Response Services Requirements & Descriptions). The following are exceptions and limitations to CRS and PRS:

i. CRS is not available for third-party libraries, integrations, or code not developed using SC or SCA.

ii. PRS is not available for third-party solutions or integrations, or any physical hardware-related issues.

iii. CRS and PRS are limited to a reproducible Severity Level 1 (Critical) issue (Customer must provide detailed instructions that allow Oracle to reproduce the specific usage that caused the Incident).

   a. Solely for purposes of CRS, Cloud Service (as defined in the Agreement) shall mean Website.

   b. Solely for purposes of PRS, Service (as defined in the Subscription Services Agreement) shall mean NSPOS

iv. Oracle may, in its sole but reasonable discretion cease to provide CRS and PRS for any Customer that has not taken appropriate or recommended actions to remediate previously reported issues.

v. Oracle may decline to provide CRS, for an individual Website-related error, or PRS, for an individual NSPOS-related error, if, in its sole but reasonable discretion, Oracle concludes that the level of effort required to address the error is not commercially reasonable.