COMMUNITY 360

Community 360 Hosting & Support Delivery Policies

Effective Date: 01st June 2024

OVERVIEW

These Community 360 Hosting and Support Delivery Policies (these “Hosting Policies”) describe the Cloud Service as defined in the Agreement (defined below). These Hosting Policies only apply if referenced in Customer’s Agreement or Estimate/Order Form. These Hosting Policies should be reviewed in conjunction with the Community 360 Exceptions to the Hosting & Support Delivery Policies (“Exceptions Policy”) which details any exceptions to these Hosting Policies. The Exceptions Policy can be found at https://www.community360.au/termsofservices.

These Hosting Policies may reference other Community 360 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 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. Community 360’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 Community 360 discretion; however, Community 360 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 Community 360 which are subject to separate terms and conditions (other than the Agreement), including but not limited to 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 in the Exceptions Policy.

DEFINITIONS

“Advanced Customer Support” is a managed service which Community 360 offers on a subscription basis. Advanced Customer Support is provided by Community 360 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 Community 360 regarding the Community 360 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 Community 360 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 Community 360 company holidays.

“Electronic Communications” means any transfer of signs, signals, text, images, sounds, data or intelligence of any nature transmitted in whole or part electronically received and/or transmitted through the Cloud Service.

“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 Community 360 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 Community 360 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 Community 360 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 Community 360 sole discretion.

I. COMMUNITY 360 CLOUD SERVICES DATA SECURITY POLICIES

For the Cloud Service procured on the applicable Order, Community 360 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 Community 360 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, Community 360 shall comply with all obligations regarding Customer Data, including, without limitation, Community 360 obligations to maintain commercially reasonable Safeguards as provided herein.

A. Community 360 Security Policy

Community 360 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 Community 360 security personnel supporting the Cloud Service.

B. Community 360 Security Organization

Community 360 has, and will continue to have, a dedicated security organization that is responsible for the ongoing monitoring of Community 360 security infrastructure, the review of Community 360 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. Community 360 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 Community 360 data and other Community 360 customers' data; and

iv. Database fields in the Cloud Service designated for credit card data information and social security numbers will be encrypted, and Community 360 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 Community 360. Customer understands that the technical processing and transmission of Customer's Electronic Communications is fundamentally necessary to use of the Cloud Service. Customer is responsible for securing DSL, cable or another high-speed Internet connection and up-to-date "browser" software in order to utilize the Cloud Service. Customer expressly consents to Community 360 interception and storage of Electronic Communications and/or Customer Data as needed to provide the Services, and Customer acknowledges and understands that Customer's Electronic Communications will involve transmission over the Internet, and over various networks, only part of which may be owned and/or operated by Community 360. Customer further acknowledges and understands that Electronic Communications may be accessed by unauthorized parties when communicated across the Internet, network communications facilities, telephone or other electronic means. Without limiting Community 360 applicable obligations under the Security or Confidentiality Sections of the Agreement, Community 360 is not responsible for any Electronic Communications and/or Customer Data which are delayed, lost, altered, intercepted or stored during the transmission of any data whatsoever across networks not owned and/or operated by Community 360, including, but not limited to, the Internet and Customer's local network.

Community 360 will use strong cryptography and security protocols consistent with industry standards, as documented in the User Guides for the Cloud Service.

E. Incident Response

Community 360 will monitor a variety of communication channels for known incidents, and Community 360 security team will react promptly to such known incidents. In the event of a Security Incident, Community 360 will: (i) notify Customer in accordance with Community 360 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 Community 360 Confidential Information.

Incidents involving Personal Information shall be managed according to the provisions set forth within the Community 360 Data Processing Agreement.

F. Change Management

Community 360 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

Community 360 servers will use a hardened operating system implementation customized for the Cloud Service. Community 360 will maintain a risk-based prioritized patch management policy.

H. Access Control and Privilege Management

Community 360 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 Community 360 personnel.

I. User Accounts: Passwords, Access and Notification

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.

Customer shall authorize access to and assign unique passwords and user names to its Users. Customer will be responsible for the confidentiality and use of User's passwords and user names. Customer will also be responsible for all Electronic Communications, including those containing business information, account registration, account holder information, financial information, Customer Data, and all other data of any kind contained within emails or otherwise entered electronically through the Cloud Service or under Customer's account. Community 360 will act as though any Electronic Communications it receives under Customer's passwords, user name, and/or account number will have been sent by Customer. Customer shall use commercially reasonable efforts to prevent unauthorized access to or use of the Cloud Service and shall promptly notify Community 360 of any unauthorized access or use of the Cloud Service and any loss or theft or

unauthorized use of any User's password or name and/or Cloud Service account numbers.

J. Community 360 Responsibilities and Policy Controls

Community 360 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

Community 360 will protect its infrastructure with multiple levels of secure network devices. All remote access to the Cloud Service environments by Community 360 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, Community 360 shall maintain PCI DSS compliance for those portions of the Cloud Service that are designated by Community 360 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, Community 360 shall ensure performance of annual third-party attestation reports completed in accordance with the AICPA and IFAC Standards for Assurance Engagements:

a. Community 360 shall ensure performance of an annual SOC 1 / ISAE 3402 Type II report.
b. Community 360 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 Community 360 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. Community 360 shall ensure performance of a third-party certification audit of Community 360 ISMS against the requirements of the ISO 27001 standard.

(iv) Customer may submit a request to their account executive for a copy of Community 360 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 Community 360 in connection with this Section I.M.iv are deemed Community 360 Confidential Information.

(v) If similar third-party audits, standards and/or certifications become available in the future, Community 360 may choose to perform such audit and/or certify to such established industry standard selected by Community 360 in place of those in this Section I.M.

N. Data Center Environments and Physical Security

The following is a general description of Community 360 various data center environments and efforts to ensure physical security in these environments.

Data centers running Cloud Services in Community 360 Cloud Infrastructure are governed by Section 1.2, "Physical Security Safeguards", and Section 2.1, "Community 360 Cloud Services High Availability Strategy", of the ***Community 360 Cloud Hosting and Delivery Policies*** which are found at www.oracle.com/contracts/cloudservices or other URL as designated by Community 360.

O. Disaster Recovery

Community 360 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 Community 360 in its sole discretion. If Community 360 determines that an event constitutes a disaster requiring execution of its Internal DR Plan, Community 360 will work to restore the production environments of the affected Cloud Service.

Recovery Time Objective: Recovery Time Objective **("RTO")** is Community 360 objective for the maximum period of time between Community 360 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 Community 360 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 Community 360). The RPO does not apply to any data loads that are underway when the disaster occurs.

Unless otherwise specified in the Exceptions Policy, (1) the RTO for the Cloud Services is 12 hours and (2) the RPO for the Cloud Services is 1 hour.

If the Cloud 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. (Community 360 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, Community 360 delivery of non-critical bug fixes and enhancement requests are suspended.

P. Risk Assessments

Community 360 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 Community 360, in its sole discretion.

Q. Handling of Personal Information

Community 360 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, Community 360 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. Sensitive Data

Customer is responsible for ensuring sensitive data (e.g., social security numbers, credit card numbers) are only stored in the appropriate designated fields for such data.

S. 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.

T. SECTION I EXCEPTIONS & EXCLUSIONS.

Please refer to the Community 360 Exceptions to the Hosting & Support Delivery Policies document found at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ for exceptions and exclusions to Section I.

II. COMMUNITY 360 SUPPORT SERVICES

A. General

Subject to Customer's procurement of Support Services (defined herein), the terms of this Section II (the "Support Terms") describe Community 360 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, Community 360 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) Community 360 shall not have any obligation to provide Support Services with respect to any:

i. 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;
ii. First Level Support, which shall be provided by Customer;
iii. Enhancement Requests; or
iv. any items excluded pursuant to Section II.E (Exclusions and Exceptions from Support Services).

(iii) Community 360 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 Community 360 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 Community 360 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 Community 360 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 Community 360 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 Community 360 prior written notice, including the relevant contact information for any new Authorized Contact.

Permitted number of qualified Authorized Contacts:

(a) Basic Support: 2

(b) Premium Support: 4

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

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

(b) Detailed instructions that allow Community 360 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. Community 360 may share such information and other information about Incidents with its contractors, vendors and/or third party application providers to support Community 360 provision of the Support Services described herein.

(iii) Severity Levels. Community 360 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. Community 360 may reclassify Incidents based on the current impact on the Cloud Service and business operations as described below. In the event Community 360 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) Community 360 Obligations. Community 360 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, Community 360 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	2Business 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) Community 360 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 Community 360 with all reasonable assistance and providing Community 360 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. SECTION II EXCEPTIONS & EXCLUSIONS.

Please refer to the Community 360 Exceptions to the Hosting & Support Delivery Policies document found at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ for exceptions and exclusions to Section II.

III. COMMUNITY 360 SERVICE LEVEL COMMITMENT

During the Term, the Cloud Service will meet the service level specified herein. If the Cloud Service fails to achieve the service level, then Customer will be entitled, as its sole and exclusive remedy, to a credit for the Cloud Service in accordance with the terms set forth herein.

A. Service Availability

Community 360 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 Community 360, and Customer was negatively impacted (attempted to log into or access the Cloud Service and failed due to Unplanned Downtime, as defined below), Community 360 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%

Community 360 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. Community 360 shall calculate any Unplanned Downtime using Community 360 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 Community 360 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 Community 360 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 Community 360 may communicate, every Saturday night between 10:00pm - 10:20pm Pacific Time is reserved for scheduled maintenance as may be needed.

Community 360, 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 Community 360 at info@community360.au 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 Community 360. 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 Community 360 and Customer must resubmit their claim in order for Community 360 to consider the request for a Service Credit. Customers with accounts that are past due or in default to Community 360 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 (Community 360 Service Level Commitment) may be amended at any time by Community 360 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:

Please refer to the Community 360 Exceptions to the Hosting & Support Delivery Policies document found at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ for exceptions and exclusions to Section III.

IV. COMMUNITY 360 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 Community 360 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. Community 360 will use commercially reasonable efforts to analyze Website-related errors and help identify causation. Community 360 will provide reasonable remediation assistance, help identify a workaround, or recommend that Customer separately procure Professional Services from Community 360. Community 360 may require access to Customer's sandbox and production environments of the Cloud Service ("Customer Accounts"). Customer agrees to provide Community 360 with the level of Customer Account(s) access that is reasonably necessary for so long as Community 360 requires such access and Customer shall immediately remove such access upon the completion of CRS activity.

Point-of-Sale Response Services. Community 360 will use commercially reasonable efforts to analyze NSPOS-related errors and help identify causation. Community 360 will provide reasonable remediation assistance, help identify a workaround, or recommend that Customer separately procure Professional Services from Community 360. Community 360 may require access to Customer's sandbox and production environments of the Cloud Service ("Customer Accounts"). Customer agrees to provide Community 360 with the level of Customer Account(s) access that is reasonably necessary for so long as Community 360 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 Community 360. Community 360 may, in its sole discretion, immediately cease to provide Response Services at any time upon notice to Customer.

D. Other

Solely for purposes of CRS, “Cloud Service” (as defined in the Agreement) shall mean “Website”. Solely for purposes of PRS, “Service” (as defined in the Agreement) shall mean “NSPOS”.

E. SECTION IV EXCEPTIONS AND EXCLUSIONS:

Please refer to the Community 360 Exceptions to the Hosting & Support Delivery Policies document found at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ for exceptions and exclusions for Section IV.