ORACLE

Oracle NetSuite
托管和支持交付政策

生效日期：2026 年 11 月 13 日

目录

Overview 4

Definitions 5

I. Oracle NetSuite Cloud Services Data Security Policies 6
- A. Oracle NetSuite Security Policy 6
- B. Oracle NetSuite Security Organization 6
- C. Data Storage and Handling 6
- D. Data Transmission 6
- E. Incident Reponse 6
- F. Change Management 7
- G. Server Operating Systems 7
- H. Access Control and Privilege Management 7
- I. User Accounts: Passwords, Access and Notification 7
- J. Oracle Responsibilities and Policy Controls 7
- K. Password Configuration 7
- L. Network Connectivity Security Requirements 7
- M. Audits and Certifications 8
- N. Data Center Environments and Physical Security 8
- O. Disaster Recovery 8
- P. Risk Assessments 9
- Q. Handling of Personal Information 9
- R. Sensitive Data 9
- S. Use of Services 9
- T. Data Retrieval and Deletion at Termination. 9
- U. SECTION I EXCEPTIONS & EXCLUSIONS. 9

II. Oracle NetSuite Support Services 10
- A. General 10
- B. Scope of Support Services 10
- C. Termination 10
- D. Incident Reporting and Response Times 10
- E. SECTION II EXCEPTIONS & EXCLUSIONS. 12

III. Oracle NetSuite Service Level Commitment 13
- A. Service Availability 13
- B. Scheduled and Unscheduled Maintenance 13
- C. Service Credit Request 13
- D. Updates 13
- E. Notice 13
- F. SECTION III EXCEPTIONS & EXCLUSIONS: 14

IV. Oracle NetSuite Response Services Requirements 15

A. General 15
B. Response Services Requirements & Descriptions 15
C. Termination 15
D. Other 15
E. SECTION IV EXCEPTIONS AND EXCLUSIONS: 15
V. Artificial Intelligence Terms & Conditions 16
A. Oracle Artificial Intelligence Terms 16
B. Open AI LLM – Additional Terms of Use 16
C. xAI LLM – Additional Terms of Use 16
VI. Statement of Changes 18

概述

这些 Oracle NetSuite 托管和支持交付政策（这些“**托管政策**”）描述了协议（定义见下文）中定义的云服务。仅当在客户的协议或报价单/订购文件中引用时，这些托管政策才适用。这些托管政策应与 Oracle NetSuite 托管和支持交付政策例外情况（“例外情况政策”）一起审查，后者详细介绍了这些托管政策的任何例外情况。例外情况政策见 https://www.oracle.com/corporate/contracts/cloud-services/netsuite/。

这些托管政策可能引用其他 Oracle Cloud 政策文件。这些托管政策或此类其他政策文件中所提及的任何“贵方”均应视为指代客户报价单/订购文件（“**订购文件**”）或协议中定义的“客户”。在这些托管政策中，(1)“协议”是指客户订购文件中引用的适用协议，该协议管理客户对云服务的使用，并引用这些政策。此外，以下条款也适用于这些托管政策：

- 这些托管政策中提及的以下术语的含义应与 NetSuite Connector 订购服务协议中规定的含义相同：(a)“客户”应包括“订户”，(b)“客户数据”应包括“订户数据”，(c)“期限”应包括“初始期限”和任何“续订期限”。
- 这些托管政策中提及的“服务期限”应指客户按照客户订购文件中的规定购买的云服务的期限（例如，12 个月）。

这些托管政策中未另行定义的粗体术语应具有协议（包括纳入协议的文件）或客户订购文件（如适用）中赋予它们的含义。

客户的订购文件或协议可能包括与特定云服务有关的其他详细信息或例外情况。云服务根据适用协议和客户订购文件的条款提供。Oracle 是否交付云服务取决于客户及客户用户对于上述文件及所纳入政策规定的客户义务和责任的履行情况。这些托管政策及其中引用的文件可由 Oracle 自行决定进行更改；但是，Oracle 政策变更不会导致在客户订购文件的服务期限内提供的云服务的性能、功能、安全性或可用性水平的实质性降低。

这些托管政策不适用于任何第三方应用程序（如协议中定义）、Oracle 销售的受单独条款和条件（除了协议之外）约束的任何服务，包括但不限于 NetSuite US Payroll Service，或客户订购文件中另行规定的服务（包括在适用的项目说明或服务说明中）。这些托管政策的其他例外情况在例外情况政策中概述。

定义

“高级客户支持”是 Oracle 根据订购方式提供的一种托管服务。高级客户支持由 Oracle 提供，以帮助客户使用云服务或云服务的特定组件。

“**替代解决方案**”是指对某个事件的解决方案或更正，其使云服务能够实质上按照用户指南运行。

“**授权联系人**”是指指定的客户员工或授权代理人，其：(i) 拥有足够的云服务技术专长、培训和/或经验，可履行客户在本政策下的义务；(ii) 负责与 Oracle 就这些托管政策的第 II 节中所述的 Oracle NetSuite 支持服务进行的所有沟通，包括案例提交和事件报告；以及 (iii) 经客户授权代表客户请求和接收云服务的支持服务。

“**基本支持**”是指本政策所述的 Oracle 的基本支持服务，包含在当前有效的云服务订购中。此外，基本支持将严重性 1 问题的服务时段扩展到 24x7。

“**工作日**”是指周一至周五的正常工作时间，不包括 Oracle 公司假期。

“**电子通信**”指全部或部分通过云服务以电子方式接收和/或传输的任何性质的符号、信号、文本、图像、声音、数据或情报。

“**增强请求**”是指客户要求超出云服务规范的范围添加功能或增强性能，并且此等添加和增强不包含在支持服务中。

“**一级支持**”是指对客户的客户、最终用户或关联公司的任何电话支持，或针对用户错误、网络错误、配置错误或互联网延迟或故障的一般解决方案。

“**帮助文档**”是指描述云服务功能的在线英语帮助中心文档，其可能不时更新。帮助文档不包含从 Oracle 以外的第三方来源获得或衍生的、任何格式的材料、内容或信息（客户可能会通过服务、在服务中或与服务的使用相关联而访问此等材料、内容或信息）。

“**事件**”是指由授权联系人报告的云服务的单个支持问题或可重现的故障，并且此等问题或故障使得云服务未在实质上符合用户指南中描述的功能和/或规范。

“**正常工作时间**”为协议上列明的客户总部地址所在时区的工作日上午 8:00 至下午 6:00。

“**高级支持**”是指 Oracle 增强级别的支持服务。除了本政策描述的基本支持服务之外，如果客户有权获得高级支持，则严重性 1 和严重性 2 问题的正常工作时间将扩展到 24x7 范围，并提供更快的回应时间目标和额外的授权联系人。

“主 DC”应指存储客户数据的主数据中心。

“**个人信息**”应与术语“个人数据”、“个人可识别信息 (“PII”)”或适用数据保护法下的同等术语具有相同含义。

“保护措施”应指物理和技术保护措施。

“安全事件”应指包含未加密信息的客户数据实际发生的或 Oracle 合理认为已经发生的针对任何未经授权的个人或实体的未经授权披露。

“**SuiteAnswers**”是指可 24x7 访问的在线支持门户。

“**支持服务**”是指 Oracle 根据本政策规定以及协议中进一步规定的条款为云服务提供的基本支持和可选高级支持服务，但不包括一级支持或增强请求。对客户的支持服务级别应由该客户采购的支持服务级别确定。支持服务以英文提供，但 Oracle 可单方自行决定以其他语言提供支持服务。

I. ORACLE NETSUITE 云服务数据安全策略

对于根据适用订购文件采购的云服务，Oracle 应保持商业上合理的管理保护措施，旨在保护客户数据的保密性和完整性。所有此类保护措施应与受保护的客户数据的重要性相称，但在任何情况下，其保护程度均不得低于 Oracle 用于保护其自身信息或具有类似重要性的数据的保护措施，或适用法律要求的保护措施。

本政策所述的保护措施在客户订购文件的服务期限内适用；但是，这些托管政策中所述的保护措施并不全面，在适用订购文件的服务期限内，随着适用第三方安全审核、合规标准和/或认证的发展/变化，此类保护措施可能会发生更改，但前提是，任何此类保护措施的更改都不会在适用订购文件的服务期限内大幅降低云服务的整体安全性。

在服务期限内，Oracle 应遵守与客户数据有关的所有义务，包括但不限于 Oracle 保持本政策规定的商业上合理的保护措施的义务。

A. Oracle NetSuite 安全策略

Oracle 已制定并将维护针对其安全组织的安全政策，该政策要求向支持云服务的 Oracle 安全人员提供包含安全培训和隐私培训的综合培训。

B. Oracle NetSuite 安全组织

Oracle 设立并将继续维护专门的安全组织，负责持续监控 Oracle 的安全架构、审查 Oracle 的产品和服务，以及响应安全事件。

C. 数据存储和处理

用于存储客户数据的存储介质或任何具有存储能力的设备（包括移动介质），将按照行业标准实践进行保护和加固，如：

i. Oracle 将维护合理的资产管理政策，以管理此类介质的生命周期（试运行、操作、维护、维修、修改、更换和停用/处置）；

ii. 包含客户数据的已停用介质将按照 NIST 800-88 中度敏感级别（或类似数据销毁标准）进行销毁；

iii. 客户数据将与 Oracle 数据和其他 Oracle 客户的数据进行逻辑分割；以及

iv. 云服务中指定用于信用卡数据信息和社会安全号的数据库字段将被加密，Oracle 不会在测试、开发或非生产环境中处理此类客户数据。

D. 数据传输

客户通过 Oracle 指定的安全通信协议访问云服务。客户理解，客户电子通信的技术处理和传输对客户使用云服务而言具有根本的必要性。客户负责取得并维护 DSL、有线或其他高速互联网连接以及最新的“浏览器”软件，以便使用云服务。客户明确同意 Oracle 在为提供服务而有必要的情况下对电子通信和/或客户数据的截取和存储，客户认可并理解，客户的电子通信将涉及通过互联网和各种网络的传输，其中只有部分网络可能是由 Oracle 拥有和/或运营的。客户进一步认可并理解，当电子通信通过互联网、网络通信设施、电话或其他电子方式进行传输时，其可能会被未经授权的他方访问。在不限制 Oracle 在协议“安全”或“保密”两节下的适用义务的前提下，若任何电子通信和/或客户数据在并非由 Oracle 拥有和/或运营的网络中（包括但不限于互联网以及客户的本地网络）传输时遭受任何延误、丢失、篡改、拦截或存储，Oracle 不对此承担任何责任。

Oracle 将使用符合行业标准的强加密和安全协议，如云服务的用户指南中所述。

E. 事件回应

Oracle 将监控各种通信渠道以查找已知事件，并且 Oracle 的安全团队将会迅速对此类已知事件做出回应。如果发生安全事件，Oracle 将：(i) 根据 Oracle 在适用法律或监管要求下的义务，在适用安全泄露法律适用于此类安全事件的范围内通知客户；以及 (ii) 在采取纠正措施后进行渗透测试（如适用），并向客户提供测试结果汇总，且该类测试结果将被视为 Oracle 保密信息。

涉及个人信息的事件应按照 Oracle 数据处理协议内规定的条款进行管理。

F. 变更管理

Oracle 将维护变更管理政策，以确保对影响信息安全的组织、业务流程、信息处理设施和系统的变更得到控制。

Oracle 可能决定将某项云服务指定为生命周期终止 ("EOL")，并公布该云服务的停用日期（“停用日期”）。在合理可行的情况下，Oracle 将至少在公布的停用日期前十二个月（“EOL 期限”），就其 EOL 指定发出通知。在 EOL 期限内，云服务仍将获得必需的技术支持和更新，包括安全补丁、错误修复和合规性更新。自停用日期起，云服务将不再普遍可用并将被停用。客户负责在停用日期之前取回其客户数据。如果 Oracle 宣布某项云服务生命周期终止，Oracle 可以指定一项后继云服务，并要求客户在停用日期之前转换到此云服务。

注意：*此政策到 2027 年 11 月 13 日才生效。*

G. 服务器操作系统

Oracle 服务器将使用为云服务定制的强化操作系统实现。Oracle 将维护基于风险的优先补丁程序管理政策。

H. 访问控制和权限管理

Oracle 采用系统和流程，根据最低权限和职责分离来限制物理和逻辑访问，以确保关键数据只能由授权的 Oracle 人员访问。

I. 用户账户：密码、访问权限和通知

客户将控制云服务中用户角色的创建、删除和暂停，如适用云服务用户指南中所述。云服务允许客户履行管理职能。

客户应授予用户访问权限、并为用户分配唯一的密码和用户名。客户将对用户密码和用户名的保密和使用负责。客户还将对所有电子通信负责，此类电子通信可能包含业务信息、账户注册、账户持有人信息、财务信息、客户数据，以及在电子邮件中包含的或以其他电子方式通过云服务或客户账户输入的任何类型的所有其他数据。Oracle 将推定，其所接收的任何使用客户的密码、用户名和/或账号的电子通信是由客户发送的。客户应采取商业上合理的措施，防止未经授权访问或使用云服务，并应及时通知 Oracle 任何未经授权的访问或使用云服务的情形，以及任何用户密码、用户名和/或云服务账号的丢失、被盗或未经授权的使用。

J. Oracle 责任和策略控制

Oracle 将采取措施，确保仅根据协议的条款和条件处理客户数据。

K. 密码配置

如适用云服务用户指南中所述，某些云服务允许客户通过云服务的可配置策略设置以及在云服务中使用单点登录功能时，应用自己的密码和身份验证策略。

L. 网络连接安全要求

Oracle 将使用多级安全网络设备保护其架构。有权访问客户数据的 Oracle 人员对云服务环境的所有远程访问都必须通过以下一种方式或组合方式进行：虚拟专用网络、多因素身份验证、相互身份验证、客户端信任评分或其他具有同等或更高安全级别的身份验证方法。

M. 审核和认证

以下安全审核和认证与云服务相关，如下所述：

i. PCI-DSS。支付卡行业数据安全标准 (“PCI DSS”) 是一项全球信息安全标准，适用于处理 Visa、Master Card、American Express 等品牌信用卡的组织。PCI 标准由银行卡品牌强制执行，并由支付卡行业安全标准委员会运行。在适用订购文件的服务期限内，Oracle 应对 Oracle 指定为用于存储和处理信用卡数据的云服务部分保持 PCI DSS 合规性。

客户有责任确保，其使用云服务存储或处理信用卡数据的行为遵守适用的 PCI DSS 要求，并且不得在云服务中存储信用卡和社会保障数据，除非是在为此类数据指定的加密字段中存储。客户或代表客户对云服务所做的任何更改都可能影响客户对 PCI DSS 要求的合规，客户应自行负责确保任何此类更改符合 PCI DSS 要求。

ii. SOC 报告证明。美国注册会计师协会 (“AICPA”) 建立了系统和组织控制 (“SOC”) 框架，用于评估和报告服务组织解决特定用户需求的控制措施的有效性。就云服务而言，Oracle 应确保根据 AICPA 和 IFAC 鉴证业务标准执行完成年度第三方证明报告：

a. Oracle 应确保执行年度 SOC 1 / ISAE 3402 类型 II 报告。

b. Oracle 应确保执行年度 SOC 2 类型 II 报告，以掌握安全性、可用性和保密性属性。

c. Oracle 管理层将通过制定和实施纠正行动计划，及时处理任何导致对 SOC 报告提出保留意见的重大发现。

iii. ISO 27001。ISO 27001 是由国际标准化组织 (“ISO”) 和国际电工委员会 (“IEC”) 发布的领先国际标准，用于衡量信息安全管理体系 (“ISMS”)。此标准规定了建立、实施、运行、监控、审查、维护和改进记录的 ISMS 的要求。

Oracle 应确保根据 ISO 27001 标准的要求对 Oracle 的 ISMS 执行第三方认证审核。

iv. 客户可以向其客户主管提交请求以获取 Oracle 的以下最终文件的副本：a) SOC 1 / ISAE 3402 类型 II 报告；b) SOC 2 类型 II 报告；以及 (c) ISO 27001 证书和适用性声明 (“SOA”)。Oracle 提供的与本 I.M.iv 节相关的任何此类报告、证书和支持文件均视为 Oracle 保密信息。

v. 如果将来可以使用类似的第三方审核、标准和/或认证，Oracle 可选择以其所选的此类公认行业标准为依据开展此类审核和/或认证，以取代本 I.M 节规定的标准。

N. 数据中心环境和物理安全

下面是对 Oracle 各种数据中心环境的一般描述，以及为确保这些环境中的物理安全所做的努力。

在 Oracle Cloud Infrastructure (“**OCI**”) 中运行云服务的数据中心受 ***《Oracle 云托管和交付政策》***（见 www.oracle.com/contracts/cloud-services 或 Oracle 指定的其他 URL）的第 1.2 节“物理安全保护措施”和第 2.1 节“Oracle 云服务高可用性策略”约束。

O. 灾难恢复

Oracle 维护有一项内部灾难恢复计划（“**内部 DR 计划**”），意图在发生 Oracle自行决定宣布的灾难时为客户的生产账户提供服务恢复能力。如果 Oracle 确定某个事件构成灾难，需要执行其内部 DR 计划，Oracle 将会努力恢复受影响的云服务的生产环境。

在灾难恢复场景中，客户数据可能会迁移至数据中心区域之外，以保持服务连续性。

恢复时间目标：恢复时间目标 **("RTO")** 是指 Oracle 在其决定激活本政策所述流程与客户可以在替代站点恢复生产运作的时间点之间的最长期限目标。如果做出激活灾难恢复流程的决定时正在进行升级，则首先启动并完成灾难恢复流程，然后再完成升级。

恢复点目标：恢复点目标 **("RPO")** 是指 Oracle 的数据丢失最长期限目标，以第一个事务丢失的时间到灾难发生的时间（Oracle 认可的时间）来衡量。RPO 不适用于灾难发生时正在进行的任何数据加载。

除非在例外情况政策中另有规定，否则 (1) 云服务的 RTO 为 12 小时，(2) 云服务的 RPO 为 1 小时。

如果云服务无法实现 RTO，客户将有权根据第 III 节中规定的条款获得使用云服务的服务储值，作为其唯一且排他性的补偿。（Oracle NetSuite 服务级别承诺）。

在灾难事件期间，客户可能会在云服务的运行中遇到一些延迟。

在主动故障转移事件或恢复操作期间，Oracle 的非关键错误修复和增强请求交付将暂停。

P. 风险评估

Oracle 应每年对云服务执行风险评估。此评估应包括对驻留在云服务上的客户数据的保密性、完整性和可用性进行的风险评估，以及一份书面计划，以纠正或缓解其安全政策中的风险，使其达到 Oracle 自行决定的可接受剩余风险水平。

Q. 个人信息的处理

Oracle 将根据适用协议处理个人信息，作为其提供服务的一部分，并负责遵守适用数据保护法规定的相应义务。在处理个人信息时，Oracle 应实施并维护适当的技术和组织安全措施，以防止意外或非法破坏、丢失、更改、未经授权披露或访问个人信息。

R. 敏感数据

客户负责确保敏感数据（例如，社会安全号、信用卡号）仅存储在此类数据的适当指定字段中。

S. 服务使用

本云服务不得向委内瑞拉境内用户提供或供此类用户访问，亦不得为了委内瑞拉境内任何个人或实体（包括但不限于委内瑞拉政府）的利益使用本云服务或服务的任何输出。

T. 终止时的数据取回和删除。

终止前，客户应在仍可访问云服务时取回其希望保留的客户数据。Oracle 将在云服务终止后 60 天（"取回期"）内应客户请求向客户提供账户访问权限，以便客户取回数据。如果客户需要 Oracle 协助取回客户数据，客户可通过其客户经理请求协助，但需支付额外费用。

云服务终止后，储存在生产云服务环境中的客户数据在取回期内保持禁用或非活动状态。取回期届满后，客户数据将排队等待删除。在取回期届满后的十 (10) 个月内，除非法律另有要求，Oracle 将删除 Oracle 维护的生产云服务环境内、用于提供报价单/订购文件中购买的云服务的所有客户数据，或使其无法访问。

U. 第 I 节例外情况和排除条款。

有关第 I 节的例外情况和排除条款，请参阅 Oracle NetSuite 托管和支持交付政策例外情况文档（见 https://www.oracle.com/corporate/contracts/cloud-services/netsuite/）。

II. ORACLE NETSUITE 支持服务

A. 概述

根据客户购买的支持服务（定义见本政策），本第 II 节的条款（“**支持条款**”）描述了 Oracle 依据协议条款和客户已采购的支持服务级别条款，向客户提供支持服务。

B. 支持服务范围

i. 根据这些支持条款，Oracle 应根据下面第 II.D 节（事件报告和回应时间）和第 II.E 节（支持服务的例外情况和排除条款）的规定，解决客户使用云服务时可能产生的所有事件。

ii. Oracle 没有义务就以下任何方面提供支持服务：

a. 客户或任何第三方对云服务进行的改编、配置或修改，包括使用 SuiteScript 或 JavaScript 进行的此等改编、配置或修改；

b. 一级支持，其应由客户提供；

c. 增强请求；或

d. 根据第 II.E 节（支持服务的例外情况和排除条款）排除的任何项。

iii. 作为云服务的一部分，Oracle 将向客户提供帮助文档和其他在线资源，以帮助客户使用云服务。

iv. Oracle 可能会提供专业服务或高级客户支持来帮助解决支持服务范围之外的问题。任何专业服务或高级客户支持服务均应根据单独的协议和/或订购文件提供，并应遵守协议和 Oracle 当时适用的咨询费用和条款。

C. 终止

即使本政策或适用协议中有任何相反的规定，这些支持条款应在协议到期或终止、或客户访问适用云服务的权利到期或终止时终止。

D. 事件报告和回应时间

i. 授权联系人。所有事件报告都必须由授权联系人向 Oracle 提交。客户报告事件的主要方法是通过 SuiteAnswers。尽管有上述规定，如果购买基本支持的客户无法访问 SuiteAnswers，则客户可以通过电话向 Oracle 通知 S1（定义见第 II.D.iii 节（严重性级别））事件。如果购买高级支持的客户无法访问 SuiteAnswers，则客户可以通过电话向 Oracle 通知 S1 和 S2（定义见第 II.D.iii 节（严重性级别））事件。客户可通过事先书面通知 Oracle 不时替换授权联系人，通知内容应包括任何新授权联系人的相关联系人信息。

允许的合格授权联系人数量

- 基本支持：2 个
- 高级支持：4 个

ii. 必要信息。所有事件报告均必须包括以下信息（如适用）：

a. 客户的标识号，作为设置的一部分提供。

b. 允许 Oracle 重现导致所报告事件的具体使用情况的详细说明。

c. 所有相关错误消息的准确描述。

d. 事件和预期结果的完整描述。

e. 发现事件时的任何特殊情况。

f. 对于 S1 事件，提供额外联络点。

Oracle 可以与其承包商、供应商和/或第三方应用程序提供商共享此类信息和有关事件的其他信息，以支持 Oracle 提供本政策所述的支持服务。

iii. 严重性级别。Oracle 将与客户合作，并根据下文定义为所有事件分配适当的严重性级别（各称**"严重性级别"**）。分配严重性级别可对报告的事件进行优先级排序。Oracle 可根据当前对云服务和业务运营的影响重新分类事件（如下文所述）。如果 Oracle 确定事件实际上是增强请求，则不应根据这些支持条款处理此等事件。严重性级别定义为：

a. **"严重性级别 1"**或**"S1（关键）"**是指事件导致客户的云服务生产使用停止或受到严重影响，以至于客户无法合理地继续业务运营。这可能会导致客户业务运营发生实质性和即时性中断，从而导致客户数据丢失和/或此类数据的可用性受限，和/或造成重大财务影响。

b. **"严重性级别 2"**或**"S2（重要）"**是指事件导致云服务的一个或多个重要功能不可用，且没有可接受的替代解决方案。客户对云服务的实施或生产使用仍会继续而不会停止；但是，客户的业务运营受到了严重影响。

c. **"严重性级别 3"**或**"S3（不太重要）"**是指事件导致：(a) 重要云服务功能不可用，但有替代解决方案可用，或 (b) 不太重要的云服务功能不可用，且没有合理的替代解决方案；客户遭受轻微的业务运营功能损失和/或实施资源受到影响，或 (c) 客户提出有关云服务基本功能的问题。此类别仅适用于购买了高级支持的客户。

d. **"严重性级别 4"**或**"S4（最低）"**是指事件对业务运营或云服务的基本功能造成极低的影响。此类别仅适用于购买了高级支持的客户。

iv. Oracle 的义务。Oracle 将在正常工作时间内提供支持服务访问权限，以便客户报告事件并获得帮助。收到事件报告后，Oracle 应确定发生的事件是否使得客户有权根据这些支持条款获得支持服务，如果是，则应：

a. 确认收到事件报告，并通知客户事件的案例编号，此后，双方在有关该事件的任何通信中都必须使用该案例编号。

b. 与客户合作，根据本政策列明的标准设置事件的严重性级别。

c. 分析事件并核实是否存在问题。

d. 根据本政策所述的条款，向客户提供解决事件的指导和帮助。

v. 回应时间目标。

	严重性级别 1	**严重性级别 2**	**严重性级别 3**	**严重性级别 4**
基本支持	2 小时	不适用[1]	不适用[2]	不适用
高级支持	1 小时	2 小时	8 小时	2 个工作日

[1] ***注：****对于在 2019 年 12 月 1 日之前购买支持的客户，S2 回应时间为 4 小时。*
[2] ***注：****对于在 2019 年 12 月 1 日之前购买支持的客户，S3 回应时间为 2 个工作日。*

vi. 客户义务。

a. Oracle 有义务根据这些支持条款提供支持服务的前提条件是，客户：

1. 支付了报告事件日期之前的所有适用支持服务费用；

2. 具有云服务的有效访问权限；

3. 向 Oracle 提供所有合理协助，并向 Oracle 提供合理必要的数据、信息和材料；

4. 采购、安装和维护访问云服务所需的所有设备、电话线、通信接口和其他硬件和软件；
5. 提供所有一级支持；
6. 提供所有授权联系人的适当联系人信息；
7. 利用 SuiteAnswers 知识库自助研究已知的解决方案；以及
8. 利用 SuiteAnswers 事件报告门户记录所有事件案例；按照第 II.D.i 节（授权联系人）中的规定，允许通过电话方式记录 S1 事件的基本支持客户和允许记录 S1 和 S2 事件的高级支持客户除外。

b. 在客户购买支持服务的初始期限和任何续订期限内，客户应为所有云服务（包括但不限于客户后续购买的任何增量许可）用户购买并维持相同级别的支持服务。为避免疑义，客户不得选择仅为其部分服务或仅为有权访问服务的部分用户购买或续订支持服务，亦不得为其部分用户购买不同级别的支持。

E. 第 II 节例外情况和排除条款。

有关第 II 节的例外情况和排除条款，请参阅 Oracle NetSuite 托管和支持交付政策例外情况文档（见 https://www.oracle.com/corporate/contracts/cloud-services/netsuite/）。

III. ORACLE NETSUITE 服务级别承诺

在服务期限内，云服务将满足本政策规定的服务级别。如果云服务无法达到服务级别，则客户将有权根据本政策规定的条款获得云服务的储值，作为其唯一且排他性的补偿。

A. 服务可用性

Oracle 承诺在适用订购文件服务期限的每个日历月份内，为客户订购的云服务提供 99.7% 的可用性，不包括计划维护时间（**"服务可用性"**）。如果在任何日历月份内，Oracle 未满足此服务可用性，且客户受到负面影响（尝试登录或访问云服务，但因计划外停机导致失败，定义见下文），Oracle 应根据云服务的月使用费提供服务储值作为唯一且排他性的补偿，具体如下：

服务可用性	**<99.7% 且 >= 99.5%**	**<99.5% 且 >= 99.0%**	**< 99.0%**
服务储值	10%	15%	25%

Oracle 通过将月测量周期内的总分钟数与任何计划外停机时间之差除以测量周期内的总分钟数，然后再乘以 100，得出一个百分比数值，以此来衡量每个日历月份的服务可用性。**"计划外停机时间"**是指云服务出现问题导致客户无法登录或访问云服务的任何时间。Oracle 应使用 Oracle 的系统日志和其他记录计算任何计划外停机时间。计划外停机时间不包括由于以下原因导致云服务不可用的任何时间：适用云服务的任何暂停或终止，或因客户和/或第三方的设备、软件、服务或其他技术（Oracle 直接控制的第三方设备或服务除外）造成的任何其他不可用性或性能问题。

B. 计划和非计划维护

在如上表所示计算服务储值时，计划维护不计为计划外停机时间。如果 (i) 已根据下文第 III.E 节（通知）所述，以及 (ii) 至少提前计划维护时间两个完整工作日沟通维护，则该维护视为"计划维护"，但 Oracle 会尽可能至少提前一周沟通计划维护事宜。计划维护通常在每个地区的正常工作时间之外进行，一般每个季度少于 15 小时。除 Oracle 可能沟通的任何其他计划维护外，太平洋时间每周六晚上的 10:00 至 10:20 之间均保留用于可能需要的计划维护。

Oracle 可自行决定关闭云服务进行非计划维护，在这种情况下，将尝试根据下文第 III.E. 节（通知）所述提前通知客户。非计划维护将包含在计划外停机时间内，并根据上述服务可用性规定进行计算。

C. 服务储值请求

要获得本政策所述的服务储值，客户必须在自未达到服务可用性的当月月底起的 30 个日历日内向 Oracle 发送电子邮件（电子邮箱为 billing@netsuite.com）申请服务储值，且客户必须按照 Oracle 的合理要求提供索赔详细信息。成功提交的任何索赔申请都将收到回复，表示已收到申请。如果客户未收到此回复，则视为 Oracle 未收到索赔，客户必须重新提交索赔，以便 Oracle 考虑服务储值申请。如果客户的账户逾期支付或拖欠应付 Oracle 的任何款项，或者逾期履行或未履行对 Oracle 的任何重大合同义务，该客户没有资格获得本服务级别承诺项下的任何服务储值。服务储值的有效期最长为自服务储值发放季度起两年。

D. 更新

Oracle 可以自行决定随时修订托管政策的本第 III 节（Oracle NetSuite 服务级别承诺）。更新将在根据下文第 III.E. 节（通知）向客户发出通知后 30 天生效。

E. 通知

通知将以下述方式提供：(a) 客户管理员登录云服务后立即在其屏幕上显示一条说明，或 (b) 通过电子邮件发送至为客户账户管理员提供的注册电子邮件地址。

F. 第 III 节例外情况和排除条款：

有关第 III 节的例外情况和排除条款，请参阅 Oracle NetSuite 托管和支持交付政策例外情况文档（见 https://www.oracle.com/corporate/contracts/cloud-services/netsuite/）。

IV. ORACLE NETSUITE 响应服务要求

A. 概述

根据下表中规定的额外要求，这些响应服务要求是对这些托管政策第 II 节所述的 Oracle NetSuite 支持服务的补充，应管理下文所述的特定响应服务（“**响应服务**”）的提供，并且仅适用于响应服务。

B. 响应服务要求和说明

	要求		
响应服务	**支持服务级别**	**严重性级别**	**云服务**
商务响应服务	高级支持	严重性级别 1（关键）	SuiteCommerce (“**SC**”) 或 SuiteCommerce Advanced (“**SCA**”)
销售点响应服务	高级支持	严重性级别 1（关键）	NetSuite POS 模块 (“**NSPOS**”)

“**商务响应服务**”或 "**CRS**" 是指使用 SC 或 SCA 创建的网站（“**网站**”）的补充英语响应服务。

“**销售点响应服务**”或 "**PRS**" 是指 NSPOS 的补充英语响应服务。

商务响应服务。Oracle 将尽商业上合理的努力，分析网站相关的错误并帮助确定原因。Oracle 将提供合理补救协助，帮助确定解决方法，或建议客户单独从 Oracle 购买专业服务。Oracle 可能需要访问客户云服务的沙盒和生产环境（“**客户账户**”）。客户同意在 Oracle 需要的前提下向 Oracle 提供合理必要的客户账户访问权限，并且客户应在 CRS 活动完成后立即删除此类访问权限。

销售点响应服务。Oracle 将尽商业上合理的努力，分析 NSPOS 相关的错误并帮助确定原因。Oracle 将提供合理补救协助，帮助确定解决方法，或建议客户单独从 Oracle 购买专业服务。Oracle 可能需要访问客户云服务的沙盒和生产环境（“**客户账户**”）。客户同意在 Oracle 需要的前提下向 Oracle 提供合理必要的客户账户访问权限，并且客户应在 PRS 活动完成后立即删除此类访问权限。

C. 终止

响应服务是 Oracle 免费提供的一项补充服务。Oracle 可自行决定在通知客户后的任何时间立即停止提供响应服务。

D. 其他

仅就 CRS 而言，“云服务”（定义见协议）应指“网站”。

仅就 PRS 而言，“服务”（定义见协议）应指“NSPOS”。

E. 第 IV 节例外情况和排除条款：

有关第 IV 节的例外情况和排除条款，请参阅 Oracle NetSuite 托管和支持交付政策例外情况文档（见 https://www.oracle.com/corporate/contracts/cloud-services/netsuite/）。

V. 人工智能条款和条件

A. Oracle 人工智能条款

《Oracle 人工智能条款》（“Oracle AI 条款”）（可在 https://www.oracle.com/contracts/cloud-services/ 在线查看，或在 https://www.oracle.com/contracts/a-z/contract-documents/ 搜索 "Oracle AI Terms"）适用于客户订购的云服务中的人工智能功能（定义见此类条款）。

B. OpenAI LLM — 附加使用条款

使用 OpenAI LLM 的前提条件是，客户认可其使用范围仅限于 SuiteAnswers 中的**《生成式 AI 功能的 LLM 对应关系》**（“AI 矩阵”）中标明为采用 OpenAI 的功能（“AI 功能”），且仅在客户使用 NetSuite 云服务期间使用这些功能。此外，客户同意，客户和客户用户均需遵守以下条款。

1. 客户理解，客户的提示内容（如数据、图像、文本）将被发送到与客户 NetSuite 云服务关联的 Oracle 托管数据中心外部的 OpenAI 端点。通过 NetSuite 云服务访问的所有 OpenAI 端点均启用“零数据保留”，即客户数据 (a) 不会被记录以供人工审查，并且 (b) 不会被保存到磁盘或被 OpenAI 保留。
2. AI 矩阵包含给定数据中心区域中 NetSuite 云服务的 AI 功能对应关系，以及相关 OpenAI 端点的位置。
3. 如果 OpenAI (i) 删除某一端点，(ii) 停止在某一区域提供端点，或 (iii) 弃用某一版本的 OpenAI LLM，Oracle 将至少提前 90 天发出通知。
4. 使用 NetSuite 云服务 AI 功能的客户用户必须位于 OpenAI 支持的国家或地区；完整的支持国家和地区列表可在 https://help.openai.com/en/articles/5347006-openai-api-supportedcountries-and-territories 查看。
5. 在不限制客户报价单/订购文件及协议中其他条款适用性的前提下，客户同意，客户不得以违反 OpenAI 政策的方式使用 OpenAI LLM，也不得在知晓的情况下放任客户用户发生此类行为，OpenAI 政策参见以下链接：特定于服务的条款 (https://openai.com/policies/service-terms)、共享和发布政策 (https://openai.com/policies/sharing-publication-policy) 以及使用政策 (https://openai.com/policies/usage-policies）。此外，客户不得在未经未成年人父母、监护人或教师同意的情况下授权或允许未成年人使用 OpenAI LLM，也不得在知晓的情况下放任客户用户发生此类行为。

如果您目前尚未成为客户且/或无权访问 SuiteAnswers，请联系您的销售代表以获取 AI 矩阵的副本。该表被视为 NetSuite 保密信息，且仅在签署保密协议后提供。

C. xAI LLM — 附加使用条款

在使用纳入了 xAI 模型的 NetSuite 云服务时，客户同意遵守《xAI 可接受使用政策》("xAI AUP")。截至《NetSuite 云服务：补充条款和条件》发布日期的 xAI AUP 如下所述。当前版本的 xAI AUP 可在 https://x.ai/legal/acceptable-use-policy 查看，并可能由 xAI 酌情更改。**我方在 NetSuite 云服务中提供访问的 xAI 模型及其输出均以“按原样”为基础提供，且无任何形式的保证或赔偿，Oracle 不承担由 xAI 模型及其输出引起或与之相关的一切责任。**

D. Gemini LLM — 附加使用条款

在使用所含嵌入式 AI 功能采用 Google Gemini 模型的 NetSuite 云服务时，客户同意，客户及客户的用户仅可将这些 AI 功能作为适用 NetSuite 云服务的一部分使用，而不得作为对任何 Google 服务、模型或 API 的独立访问而使用。客户同意遵守《Google Cloud 可接受使用政策》("Google AUP") 和《Google 生成式 AI 禁止使用政策》("Google AI PUP")。截至本《NetSuite 托管和支持交付政策》发布日期的 Google

AUP 和 Google AI PUP 如下所述。当前版本的 Google AUP 和 Google AI PUP 可供查看，并可能由 Google 酌情更改。我方在 NetSuite 云服务中提供访问的 Google Gemini 模型及其输出均以“按原样”为基础提供，且无任何形式的保证或赔偿，我方不承担由 Google Gemini 模型及其输出引起或与之相关的一切责任。

客户及客户的用户不得使用 Google 支持的 AI 功能、Google 模型、Google AI/ML 服务或生成式输出开发竞争性或类似的产品或服务；替代、取代或规避 Google 模型；创建或改进与 Google 模型类似的模型；执行模型蒸馏或强化学习；生成合成数据以开发、训练或改进实质上与 Google AI 系统类似的 AI 系统；将 Google 输出从 Oracle、客户、客户的用户、供应商或第三方数据中分离出来，以训练或改进直接与 Google AI/ML 服务或基础模型竞争的模型；对 Google AI/ML 服务、Google 软件或 Google 模型的任何组件进行逆向工程或提取（例如使用提示词来发现训练数据）；绕过或修改安全过滤器、来源引用、指令或合规管控工具；在面向 18 岁以下人员或可能由其访问的服务中使用该功能；或将该功能用于被禁止、非法、高风险、临床、医疗建议、应急响应或受监管的用途，除非明确允许。

对于涉嫌或实际不合规的情形，Oracle 可暂停、限制、隔离或终止访问。

VI. 变更声明

日期	变更的节	变更
2025 年 10 月 3 日	第 V 节	添加了第 V 节（“人工智能条款”）
2025 年 12 月 15 日	第 V 节	添加了“OpenAI LLM — 附加使用条款”
2026 年 3 月 16 日	第 V 节	添加了“xAI LLM — 附加使用条款”
2026 年 6 月 15 日	定义 第 II.B. 节	在“定义”一节添加了“帮助文档”的定义 新增第 (iii) 小节
2026 年 11 月 13 日	第 V 节 第 I.F. 节 第 I.O. 节	添加了“Gemini LLM — 附加使用条款” 添加了“生命周期终止”政策条款。 更新了“灾难恢复”条款。