

**AGENDA PLACEMENT FORM**

(Submission Deadline – Monday, 5:00 PM before Regular Court Meetings)

Date: 08-16-2024  
Meeting Date: 08-26-2024  
Submitted By: Jim Simpson Asst. Co. Atty  
Department: \_\_\_\_\_  
Signature of Elected Official/Department Head:  
\_\_\_\_\_

<b>Court Decision:</b> <small>This section to be completed by County Judge's Office</small>
 <b>August 26, 2024</b>

**Description:**

Consider and Approve for County Judge to Sign Oracle NetSuite Ordering Document, Oracle Professional Services Ordering Document and NASPO Value Point Amendment One to the Participating Addendum; said documents being Additional and Amending Documents for Transaction Approved with Oracle on August 12, 2024.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(May attach additional sheets if necessary)

Person to Present: Steve Watson

(Presenter must be present for the item unless the item is on the Consent Agenda)

Supporting Documentation: (check one)     PUBLIC     CONFIDENTIAL

(PUBLIC documentation may be made available to the public prior to the Meeting)

Estimated Length of Presentation: 10 minutes

Session Requested: (check one)

Action Item     Consent     Workshop     Executive     Other \_\_\_\_\_

Check All Departments That Have Been Notified:

County Attorney     IT     Purchasing     Auditor  
 Personnel     Public Works     Facilities Management

Other Department/Official (list) \_\_\_\_\_

**Please List All External Persons Who Need a Copy of Signed Documents  
In Your Submission Email**



**AMENDMENT ONE TO THE PARTICIPATING ADDENDUM**

This Amendment One (this "Amendment One") amends the Participating Addendum effective August 12, 2024, by and between Johnson County, TX ("You", "Participating Entity", or "State") and Oracle America, Inc. ("Oracle" or "Contractor") (the "Participating Addendum", "PA", or "Addendum", Oracle reference number US-GMA-1301562 (AR2487)\_PA\_JohnsonTX), to the NASPO ValuePoint Master Agreement for Cloud Solutions, effective March 1, 2017 (contract # AR2487, the "Master Agreement").

The parties agree to amend the PA as follows:

1. Add a new section 9 (Governing Law and Venue) to the PA as follows:

"9. Governing Law and Venue: This Addendum will be governed by and construed according to the laws of the State of Texas. Venue for any action or claim arising out of the Addendum must be in the state courts of competent jurisdiction in or for Johnson County, Texas or the federal courts in or for Dallas County, Texas."

Subject to the modifications herein, the PA shall remain in full force and effect.

The Effective Date of this Amendment One to the Participating Addendum is \_\_\_\_\_ (to be completed by Oracle)

Johnson County, TX

Authorized Signature: *Christopher Boedeker*

Name: Christopher Boedeker

Title: County Judge

Signature Date: 8-26-2024

Oracle America, Inc.

Authorized Signature: \_\_\_\_\_

Name: Dapo Lawal

Title: Contracts Manager, Deal Mgmt.

Signature Date: 16-Aug-2024 | 9:05 AM PDT

DocuSigned by:  
*Dapo Lawal*  
CFEB048A0EA14D5...

**APPROVED AS TO FORM AND CONTENT:**

**JOHNSON COUNTY:**

*Christopher Boedeker*  
Christopher Boedeker  
As Johnson County Judge

8-26-2024  
Date

Attest: *April Long*  
County Clerk, Johnson County



8-26-2024  
Date

**ORDERING DOCUMENT**

Oracle America, Inc.  
 500 Oracle Parkway  
 Redwood Shores, CA  
 94065

<b>Name</b>	Johnson County	<b>Contact</b>	Steven Watson
<b>Address</b>	2 N Main St 120 CLEBURNE TX 76033	<b>Phone Number</b>	+1 (817) 556-6360
		<b>Email Address</b>	swatson@johnsoncountytexas.org

**New Subscription**

Services Period: 60 months						
Cloud Services	Data Center Region	Quantity	Term	Unit Net Price	Net Fee	
B94583 - Oracle NetSuite for Government Cloud Service, Standard Edition - Hosted Environment	NORTH AMERICA	1	60 mo	4,200.00	252,000.00	
B108187 - Oracle NetSuite for Government Cloud Service, Bill Capture - Each	NORTH AMERICA	1	60 mo	299.50	17,970.00	
B94584 - Oracle NetSuite for Government Cloud Service, Additional General User - Hosted Named User	NORTH AMERICA	159	60 mo	24.50	233,730.00	
B94587 - Oracle NetSuite for Government Cloud Service, Additional Planning and Budgeting User - Hosted Named User	NORTH AMERICA	11	60 mo	60.00	39,600.00	
B94590 - Oracle NetSuite for Government Cloud Service, Premium Service Tier - Each	NORTH AMERICA	1	60 mo	2,499.50	149,970.00	
B94592 - Oracle NetSuite for Government Cloud Service, Sandbox Environment - Each	NORTH AMERICA	1	60 mo	249.50	14,970.00	
B94593 - Oracle NetSuite for Government Cloud Service, Additional Sandbox Refresh - Each	NORTH AMERICA	1	60 mo	249.50	14,970.00	
B95922 - Oracle NetSuite for Government Cloud Service, Payroll - 5 Employees	NORTH AMERICA	227	60 mo	32.50	442,650.00	
<b>Subtotal</b>					<b>1,165,860.00</b>	

Fee Description	Net Fee
Cloud Services Fees	1,165,860.00
<b>Net Fees</b>	<b>1,165,860.00</b>
<b>Total Fees</b>	<b>1,165,860.00</b>

## **A. Terms of Your Order**

### **1. Applicable Agreement:**

a. This ordering document incorporates by reference the NASPO ValuePoint Master Agreement US-GMA-1301562 (AR2487) by and between Oracle America, Inc. ("Oracle") and the State of Utah, as the lead state, and the Participating Addendum US-GMA-1301562 (AR2487)\_PA\_JohnsonTX by and between Oracle and County of Johnson (collectively, the "Agreement")

### **2. Cloud Payment Terms:**

a. Net 30 days from invoice date

### **3. Cloud Payment Frequency:**

a. Quarterly in Arrears

### **4. Currency:**

a. US Dollars

### **5. Offer Valid through:**

a. 31-AUG-2024

### **6. Service Specifications**

a. The Service Specifications applicable to the Cloud Services and the Consulting/Professional Services ordered may be accessed at <http://www.oracle.com/contracts>.

### **7. Services Period**

a. The Services Period for the Services commences on the date stated in this order. If no date is specified, then the "Cloud Services Start Date" for each Service will be the date that you are issued access that enables you to activate your Services, and the "Consulting/Professional Services Start Date" is the date that Oracle begins performing such services.

## **B. Additional Order Terms**

### **1. Optional Renewal Period**

You shall have the option to renew the same services listed in the table above section A at the same usage limits for one (1) additional 60-month renewal period ("Option Renewal Period") for the total net fee of \$1,352,843.61, which shall be the sum of the following annual amounts:

- Option Year 1 \$270,568.72
- Option Year 2 \$270,568.72
- Option Year 3 \$270,568.72
- Option Year 4 \$270,568.72
- Option Year 5 \$270,568.72

Professional Services are not included in the Option Renewal Period.

The cloud services listed in the tables above section A may not be renewed at the Option Renewal Period pricing specified above if (i) Oracle is no longer making such cloud services generally available to customers, or (ii) You are seeking to cancel or reduce the number of user licenses of the cloud services specified in this ordering document.

### **2. Linking Language**

You acknowledge and agree that the terms and conditions of this document are contingent upon the simultaneous execution of the US-GMA-1301562 (AR2487)\_PA\_JohnsonTX between the parties (the "Contingent Document(s)"). If the parties do not simultaneously execute the Contingent Document with this document, then this document shall be deemed to have no legal effect, even if executed.

### **3. Non-Appropriation**

In the event funds are not appropriated for a new fiscal year period, You may terminate this order immediately without penalty or expense; provided, however, that: (a) for each of the 12-month terms of the order, You must provide a purchase order, and (b) Your issuance of each 12-month purchase order shall signify to Oracle that all funds for the given 12-month term have been fully appropriated and encumbered. Notwithstanding the foregoing, You agree to pay for all Services performed by Oracle prior to Oracle's receipt of Your notice of non-appropriation.



APPROVED AS TO FORM AND CONTENT:

JOHNSON COUNTY:

Ch Boeder  
Christopher Boedeker  
As Johnson County Judge

8-26-24  
Date

Attest: April Lung  
County Clerk, Johnson County

8-26-24  
Date



Oracle America, Inc  
COMPAN

DocuSigned by:  
Mike Estrada  
Authorized Representative of Company

16-Aug-2024 | 7:06 AM PDT  
Date

Printed Name: Mike Estrada

Title: NAMER Sr Contracts Manager

**BILL TO / SHIP TO INFORMATION**

Bill To		Ship To	
Customer Name	Johnson County	Customer Name	Johnson County
Customer Address	2 N Main St 120 CLEBURNE TX 76033	Customer Address	2 N Main St 120 CLEBURNE TX 76033
Contact Name	Steven Watson	Contact Name	Steven Watson
Contact Phone	+1 (817) 556-6360	Contact Phone	+1 (817) 556-6360
Contact Email	swatson@johnsoncountytexas.org	Contact Email	swatson@johnsoncountytexas.org



PROFESSIONAL SERVICES ORDERING DOCUMENT

Ordering Document Number: US-17222462

Oracle America, Inc. 500 Oracle Parkway Redwood Shores, CA 94065	<b>Your Name:</b> Johnson County <b>Your Address:</b> 2 North Main Street 120 Cleburne, TX 76033
--	--

<b>Oracle Representative:</b>	Thomas Hackett	<b>Your Billing Contact:</b>	Steven Watson
<b>Address:</b>	368 9th Avenue, New York-10001	<b>Address:</b>	2 North Main Street 120 Cleburne, TX 76033
<b>Phone Number:</b>	518-448-8174	<b>Phone Number:</b>	817-556-6360
<b>Email Address:</b>	thomas.h.hackett@oracle.com	<b>Email Address:</b>	swatson@johnsoncountytexas.org

You have ordered the Services listed in the table below and detailed in the attached exhibit(s), which are incorporated herein by reference.

Services	Reference	Fees	Estimated Expenses	Total Fees and Estimated Expenses
Time and Materials Services	Exhibit 1	\$434,271.00	\$43,427.00	\$477,698.00
<b>Total Fees and Estimated Expenses</b>				<b>\$477,698.00</b>

A. TERMS

- Applicable Master Agreement:** This ordering document incorporates by reference the NASPO ValuePoint Master Agreement US-GMA-1301562 (AR2487) by and between Oracle America, Inc. ("Oracle") and the State of Utah, as the lead state, and the Participating Addendum US-GMA-1301562 (AR2487)\_PA\_JohnsonTX by and between Oracle and Johnson County (collectively, the "Master Agreement"). You acknowledge and agree that the terms and conditions of this ordering document are contingent upon the execution of the Master Agreement between the parties on or prior to the last signature date of this ordering document. If the parties do not execute the Master Agreement on or prior to the last signature date of this ordering document, then this ordering document shall be deemed to have no legal effect, even if executed.
- Professional Services Delivery Policies:** The Oracle Professional Services Delivery Policies and documents incorporated therein ("Policies") apply to and are incorporated into this order. The Policies, current as of the ordering document effective date, are attached hereto as Appendix 1. Oracle's Professional Services Delivery Policies are subject to change, but such changes will not materially reduce the level of performance, functionality, security or availability for the Services, or impose additional material obligations on You with respect to this order, for the duration of Your order. The parties agree that Oracle will not provide access to third-party collaboration tools.
- Payment Terms:** Net 30 days from invoice date.
- Currency:** US Dollars.
- Offer Valid through:** 31-Aug-2024.
- Service Specifications:** The Service Specifications shall include any exhibit(s) attached to this order (including referenced or incorporated Oracle documents) and the Policies.
- Order of Precedence:** In the event of any inconsistencies, priority shall be established in the following descending order: (a) any exhibit(s) attached to this order; (b) this order; (c) the Policies; and (d) the Master Agreement.

8. **Rights Granted:** Upon payment, You have the non-exclusive, non-assignable, royalty-free, worldwide, limited right to use the services and anything developed and delivered by Oracle under this order ("services and deliverables") for Your internal business operations. You may allow Your agents and contractors to use the services and deliverables for Your internal business operations, and You are responsible for their compliance in such use. The services and deliverables may be related to Your right to use cloud or hosted/managed services or Products owned or distributed by Oracle which You acquired under a separate order. The agreement referenced in that order shall govern Your use of such services or Products, and nothing in this order is intended to grant a right to use such services or Products in excess of the terms of that order, such as the services period or number and type of environments specified in a cloud or hosted/managed service order.

You retain all ownership and intellectual property rights to Your confidential and proprietary information that You provide to Oracle under this order.

**B. ADDITIONAL ORDER TERMS**

1. When services will be performed on-site at customer location in the US, as required by US Department of Labor regulations (20 CFR 655.734), You will allow Oracle to post a notice regarding Oracle H-1B employee(s) at the work site prior to the employee's arrival on-site.

<b>APPROVED AS TO FORM AND CONTENT:</b>	
<b>Johnson County</b>	<b>Oracle America, Inc.</b>
Authorized Signature: <u></u>	Authorized Signature: <u></u>
Name: <u>Christopher Boedeker</u>	Name: <u>Gregg Bartoshek</u>
Title: <u>as Johnson County Judge</u>	Title: <u>Contract Specialist</u>
Signature Date: <u>8-26-24</u>	Signature Date: <u>16-Aug-2024   8:16 AM PDT</u>
Ordering Document Effective Date: _____	<i>{to be completed by Oracle}</i>

Attest:

  
 County Clerk, Johnson County





Your Name: **Johnson County**  
 Ordering Document Number: **US-17222462**  
 Exhibit Number: **1**

1. Description of Services.

Oracle will provide You with up to three hundred seventy-eight (378) person days of technical and functional Services to assist with the cloud enablement of Oracle NetSuite for Government Cloud Service ("NetSuite for Government") (the "Services"). Oracle will assist You in the following phases:

A. Phase 1 – Finance:

1. Focus Phase:

- a. Conduct one (1) project kick-off workshop for up to two (2) person days for Your project team to review the project governance processes and complete strategy sessions including:
  - 1. Scope management process;
  - 2. Risk management process;
  - 3. Issue management process;
  - 4. Communications management process;
  - 5. Configuration management process;
  - 6. Quality management process;
  - 7. Review the welcome packet;
  - 8. Data conversion strategy session;
  - 9. Integration strategy session; and
  - 10. Workflow strategy session.
- b. Create and provide an initial project work plan, which will include the following:
  - 1. Tasks; estimated start and end dates, and estimated durations;
  - 2. Assigned resources from You and Oracle; and
  - 3. Known dependencies.

2. Refine Phase:

- a. Conduct up to six (6) "Finance Data Migration Workshops" for up to two (2) hours each for Your project team to review the following processes for the NetSuite for Government:
  - 1. Chart of accounts ("COA") setup and fund management;
  - 2. Entity setup;
  - 3. Account balances;
  - 4. Historical data;
  - 5. Current fiscal year data import; and
  - 6. Fixed assets.
- b. Document the findings from each Finance Data Migration Workshop in a Finance Migration Engagement Report.
- c. Assist with the loading of Your finalized datasets for Finance as follows:

Finance Functional Area	Years of finalized datasets to be loaded
Journals	Five (5)
Budget	Five (5)
Purchasing and Accounts Payable	Five (5)
Projects	Five (5)
Grants	Five (5)
Accounts Receivable	Five (5)
Fixed Assets	Five (5)
Inventory	Five (5)



- d. Conduct up to six (6) "Finance Configuration Workshops" for up to two (2) hours each for Your project team to review the following processes:
  - 1. System administration;
  - 2. Planning and budgeting;
  - 3. Integrations;
  - 4. Analytics and reports;
  - 5. Workflows and automation; and
  - 6. Bill Capture.
- e. Document the findings from each Finance Configuration Workshop in a Finance Configuration Engagement Report.
- f. Configure NetSuite for Government hosted environment based upon the Finance Configuration Engagement Reports.
- g. Provide up to thirty-eight (38) total person days of guidance on configuring integrations to the following third-party applications:

Name of third party	Type of data	One-way Import/Export / Bidirectional	Frequency	Method (Application Programming Interface ("API") / Flat file)
Odyssey Court	Transaction	One-way Import	Daily	Flat file
Kofile	Revenue	Bidirectional	Real-Time	API
ComDev	Revenue	Bidirectional	Real-Time	API
Certified Payments	Payment	Bidirectional	Real-Time	API
First Financial Bank (bank statements)	Transaction	One-way Import	Daily	Flat file

- h. Configure up to one (1) of each of the following form templates to include Your information (logo, legal name, address, bill-to address, ship-to address, bank information etc.):
    - 1. Invoice;
    - 2. Purchase Order; and
    - 3. Accounts Payable check.
3. Enable Phase:
- a. Conduct up to five (5) functional training session(s) of up to two (2) hours each for Your project team on the NetSuite for Government Finance module.
  - b. Create a testing plan with You.
  - c. Provide up to four (4) person days over the course of six (6) weeks to assist with Finance user acceptance testing ("UAT").
4. Live Operate Phase:
- a. Conduct one (1) "Final Data Migration Workshop" for up to two (2) hours to complete final Finance data cutover.
  - b. Provide up to eight (8) person days of consulting post go-live support to be used within the first thirty (30) calendar days immediately following production go-live for Finance.
  - c. Facilitate the transition from Your implementation team to the NetSuite for Government support team for the Finance module.

**B. Phase 2 – Human Resources ("HR")/Payroll:**

1. Focus Phase:
- a. Conduct one (1) business process review session for up to three (3) person days for Your project team to review the following:
    - 1. Current human resources processes;
    - 2. Current payroll process;
    - 3. Changes to process updates; and
    - 4. Data conversion plan.

2. Refine Phase:

- a. Conduct up to four (4) HR/Payroll Data Migration Workshops for up to two (2) hours each for Your project team to review the following processes for the NetSuite for Government:
  - 1. System configuration and configuration of HR and payroll table data;
  - 2. Load employee data;
  - 3. Data review and clean up; and
  - 4. Load and test data changes.
- b. Document the findings from each HR/Payroll Data Migration Workshop in an HR/Payroll Data Migration Engagement Report.
- c. Assist with the loading of Your finalized datasets for HR/Payroll as follows:

Functional Area	Calendar years of finalized datasets to be loaded
Employees	Five (5)
Payroll	Five (5)

- d. Conduct up to three (3) "HR/Payroll Configuration Workshops" for up to two (2) hours each for Your project team to review the following processes:
  - 1. Timecards;
  - 2. Payroll calculations; and
  - 3. Payroll configuration.
- e. Document the findings from each HR/Payroll Data Configuration Workshop in a HR/Payroll Configuration Engagement Report.
- f. Configure NetSuite for Government hosted environment based upon the HR/Payroll Configuration Engagement Reports.

3. Enable Phase:

- a. Conduct up to seven (7) functional training session(s) of up to two (2) hours each for Your project team on the NetSuite for Government HR/Payroll module.
- b. Provide up to eighteen (18) person days to assist with up to three (3) HR/Payroll parallel tests.

4. Live-Operate Phase:

- a. Provide up to four (4) person days of consulting post go-live support to be used within the first thirty (30) calendar days immediately following production go-live for HR/Payroll.
- b. Facilitate the transition from Your implementation team to the NetSuite for Government support team for the HR/Payroll module.

C. Phase 3 – NetSuite Planning and Budgeting ("NSPB"):

1. Focus Phase:

- a. Conduct one (1) business process review session for up to two (2) hours to review the following:
  - 1. Current budgeting processes;
  - 2. Changes to process updates;
  - 3. Budget reporting needs;
  - 4. Confirm administrator access; and
  - 5. Project timeline considerations.

2. Refine Phase:

- a. Import up to one thousand (1,000) pre-defined, active general ledger ("GL") dimension members from NetSuite for Government into the NSPB instance for each of the following:
  - 1. COA;
  - 2. Funds;
  - 3. Departments;
  - 4. Projects; and
  - 5. Grants.

- b. Migrate up to five (5) years of historical income statements and balance sheets, and prior year budget data, from NetSuite for Government into the NSPB instance.
    - 1. Set up a schedule to import trial balances on a recurring basis from NetSuite for Government into the NSPB instance using standard saved searches.
  - c. Conduct up to five (5) "NSPB Configuration Workshops" for up to one and a half (1.5) hours each for Your project team to review the following:
    - 1. Web forms;
    - 2. Reports;
    - 3. Dashboards; and
    - 4. Business rules.
  - d. Document the findings from each NSPB Configuration Workshop in a NSPB Configuration Engagement Report.
  - e. Configure NSPB hosted environment based upon the NSPB Engagement Reports.
3. Enable Phase:
- a. Conduct up to one (1) functional training session(s) of up to two (2) hours each for Your project team on the NetSuite Planning and Budgeting module.
4. Live-Operate Phase:
- a. Provide up to one (1) person day of consulting post go-live support to be used within the first thirty (30) calendar days immediately following production go-live for NetSuite Planning and Budgeting.
  - b. Facilitate the transition from Your implementation team to the NetSuite for Government support team for NetSuite Planning and Budgeting module.
2. Rates, Estimated Fees and Expenses, and Taxes.
- A. The Services are performed on a time and materials ("T&M") basis; that is, You shall pay Oracle for the actual time spent performing the Services, plus materials, taxes, and expenses.
  - B. Rates. For a period of eighteen (18) from the ordering document effective date, the Services will be provided at the rates of \$143.46 per hour. Thereafter, unless otherwise agreed by You and Oracle in an amendment, the Services will be provided at Oracle's consulting rates in effect when the Services are performed.
  - C. Estimated Fees and Expenses. All fees and expenses will be invoiced monthly. The fee and expense estimates specified in Your order are intended only to be for Your budgeting and Oracle's resource scheduling purposes, and may exceed the specified totals; these estimates do not include taxes. Once fees for Services reach the estimate, Oracle will cooperate with You to provide continuing Services on a T&M basis.
3. Project Management. You and Oracle each agree to designate a project manager who shall work together to facilitate an efficient delivery of the Services.
4. Your Cooperation.
- A. Prior to the commencement of Services, designate and identify a project sponsor and a project manager that will be responsible for coordinating Your participation in this project and provide on-going support for Your implementation of the NetSuite hosted environment. Responsibilities include but are not limited to:
    - 1. Provide user feedback during configuration and validation.
    - 2. Be available as needed during the project to answer Oracle's questions, provide business decisions and other items as required.
    - 3. Provide on-going support to internal users following the implementation.
  - B. Enable administrator access to allow provisioning of Your NetSuite for Government hosted environment prior to the commencement of Services.
  - C. Modify Your processes as necessary to align with the standard functionality of NetSuite for Government.
  - D. Complete and return the questionnaire in the NetSuite for Government welcome packet to Your Oracle project manager prior to the project kick-off workshop.
  - E. Be responsible for choosing Your desired form templates from the samples provided to You during the project kick-off workshop.

- F. Make Your existing procedure and business process documentation available to Oracle at least two (2) weeks prior to the Configuration Workshop.
  - G. Notify Oracle within two (2) business days about any inaccuracies or incomplete information in project documentation provided by Oracle to You.
  - H. You will accept Oracle NetSuite release upgrades.
  - I. You will not film or record Oracle's delivery of Services, Oracle resources, or any Oracle materials.
  - J. You are responsible for planning, executing, and managing all aspects of end-to-end and final reviews, including customizing the Oracle provided templates to prepare and execute test cases and plans and reviewing test results.
  - K. Ensure that Your designated Learning Cloud Support passholder training attendee(s) are completing any implementation training courses assigned to them by the Oracle team in the timeline specified as mutually agreed by You and received from the Oracle at the start of the implementation.
  - L. Develop any necessary end-user documentation, including, but not limited to, documenting specific business practices, data examples and organization/end-user specific policies and procedures.
  - M. Manage the post-production maintenance and support of Your NetSuite for Government hosted environment.
  - N. Integration-related cooperation:
    - 1. For each third-party listed in Section 1.A.2.g, You must provide integration specifications, third-party requirements, and have a live operating environment in place in order for the implementation team to deliver the Services.
    - 2. You will be live in production on all of Your third-party applications to be integrated with NetSuite for Government at least six (6) months prior to the planned go-live date of this implementation.
    - 3. Implement and maintain the production and consumption of the file-based interfaces with Your existing systems.
  - O. Migration-related cooperation:
    - 1. Be responsible for extracting the data from Your legacy system(s), providing it in the format specified by Oracle, and assisting Oracle resources to complete data cleansing and mapping within three (3) weeks from the project kickoff call.
    - 2. Audit Your data for data migration, including historical years up through the current fiscal year.
    - 3. Financial data to be migrated must include the following:
      - a. Balances of fully qualified accounts (e.g., Fund-Dept-Obj, and other segments).
      - b. All general ledger impacting transactions (trial balance details), summed and compared by each fully qualified account to the provided balances; no transactions are omitted.
      - c. Transaction details such as purchase orders, bills, invoices, credits, voids, adjustments, payments, checks, wires, etc. must identify which general ledger impacting transaction it is associated with. The values of these details are compared to the general ledger impacting transaction totals to validate that no details are omitted.
    - 4. Human Resources and Payroll data to be migrated must include the following:
      - 1. Employees includes demographics, benefits, position, contribution/deduction assignments.
      - 2. All regular active and termed employees for the calendar year(s) in Section 1.B.2.c.
      - 3. Current year taxes, direct deposits, and leave plans for active employees.
      - 4. Payroll check history data consists of employee pay for purposes of reporting (i.e., 941, W2's, and monthly state reporting).
    - 5. Validate the final list data and transactional data within two (2) weeks from data upload.
5. Project Assumptions.
- A. A person day is defined as one (1) resource working up to eight (8) hours.
  - B. Standard functionality is defined as the functionality described in applicable documentation, for the NetSuite for Government application, provided by Oracle.
  - C. Hosted environment is defined as the combination of systems and supporting resources to which Oracle grants You access as part of the services ordered by You, that are (i) configured for the Oracle Programs operating on it and for specific uses as part of the services, and (ii) used by Oracle to perform the Services. The hosted environment consists of the production environment, and any non-production environment(s), as referenced in the applicable ordering document and Services policies.
  - D. The implementation methodology for the Services is the Oracle True Cloud Method ("TCM").



- E. The NetSuite for Government standard chart of accounts segmentation structure will be used as a default segmentation with localization as required.
- F. Integration-related assumptions:
1. If the effort to implement the third-party integrations identified by You exceeds the estimates in Section 1.A.2.g such adjustments shall be subject to the change control process.
  2. Except to the extent expressly stated in the Description of Services section of this document, the use of the terms "integrate" and "integration" throughout this document is not intended to mean that Oracle will ensure (i) the physical or functional integration of Oracle products with external legacy systems, third party products and/or other software applications; (ii) the functioning of Oracle products as a coordinated whole with such external legacy systems, third party products and/or other software applications; or (iii) any non-standard integration between Oracle products. Rather, the terms are used to refer to the overall concept of data exchange between the Oracle products and other systems, products or applications identified in this document, and may include interfacing and/or other methods of integration or interoperation as described in the Description of Services section of this document.
- G. Migration-related assumptions:
1. Data migration is limited to the assistance described in Section 1.A.2.c, Section 1.B.2.c, and Section 1.C.2.b.
  2. Data provided by Your organization will be validated by the Oracle Local Government implementation team before being loaded into NetSuite for Government. However, any discrepancies or inconsistencies will be returned to You for correction or clarification, up to three (3) revisions. It is recommended that data validation occur prior to submission of the finalized dataset for loading.
  3. Changes to HR and Payroll configuration or finalized datasets for HR and Payroll may only be made prior to the first payroll parallel test.
  4. The amount of time required to import legacy transactions and associated detail is determined by Your ability to provide reconciled data in the format requested. Delays may impact key implementation dates, including go-live.
  5. A finalized dataset for finance is defined as up to one (1) years' worth of historical data containing all the information that You wish to migrate, as validated by Your project team. Modifying the structure of the data can cause delays in the migration process and/or inconsistencies in the final result. This dataset should have all relevant details comprising the debits and credits against each accounting segment that impacts the general ledger. All transaction lines should be rounded to two (2) decimal places while maintaining balanced debits and credits and aligning with balances for each fiscal year. All transaction detail records (e.g., vendor bills, checks, accounts receivable invoices, cash receipts) must include an associating reference to the general ledger impacting transaction as well its relationship with other detail transactions such as bills-to-purchase orders or checks-to-bills. Subledger transactions details (i.e., subledger project transaction details) should be free of conflicts from their associated general ledger impact transaction.
  6. A finalized dataset for HR is defined as up to one (1) years' worth of employee data containing all employee assignments and table records for the assignments. This will include positions, deductions, benefits, taxes, and demographic information per each individual employee to be migrated over. Modifying the structure of the data can cause delays in the migration process and/or inconsistencies in the final result. All employee data should be verified by Your project team as accurate and associated with the appropriate table definitions for each of the respective areas (position details, benefit tables, etc.).
- H. The following are not included in the scope of, or fees for, Services under this exhibit:
1. Performance testing, tuning, or any management of performance.
  2. Testing beyond the activities described in this exhibit.
  3. Customizations to NetSuite for Government.
  4. Oracle Cloud subscription services.
  5. Languages other than U.S. English.
  6. Integrations or data conversions beyond what is explicitly described in this exhibit.
  7. Form configuration beyond what is explicitly described in this exhibit.
  8. Cloud middleware, database, operating and other hardware activities.
  9. Oracle transactional business intelligence training.
  10. Complex business processing or orchestration related to integrations.
  11. Transformations or data mapping of elements.
  12. Additional workforce structures for future use, expansion, or acquisitions.
  13. Extensions, customizations, or custom reports.
  14. Localizations other than those made to the chart of accounts structure.

15. Post-production Services exceeding the person days in Section 1.A.4.b, Section 1.B.4.a, and Section 1.C.4.a or thirty (30) calendar days after go-live for the respective module, whichever comes first.
16. Anything not expressly listed in the Description of Services.

ORACLE

# Oracle Professional Services Delivery Policies

Effective Date: August 2, 2024; Version 3.0

These Professional Services Delivery Policies (“Policies”) apply to the consulting services, customer success services, and managed services You ordered (“Services”). These Policies do not apply to Oracle Cloud Services. Oracle may update these Policies and the documents referenced herein; however, Oracle updates will not result in a material reduction in the level of performance, functionality, security, or availability of the Services, or in a material increase in the level of Your cooperation, for the duration of Your order.

### **ON-SITE SERVICES**

You and Oracle must agree upon the performance of the Services at one of Your facilities, taking into consideration all applicable laws, regulations, standards, and protocols. If agreed upon, You must provide a safe and healthy workspace for all Oracle resources (e.g., free from recognized hazards that cause, or are likely to cause, serious physical harm or death, and with acceptable ventilation, oxygen concentration and sound levels, and ergonomically correct workstations).

If the performance of on-site Services becomes negatively impacted due to a declared disaster, public health or safety concern, or national or global emergency, Oracle and You shall cooperate in good faith to review such impact and, if necessary, invoke the change control process.

If requested, Oracle resources will obtain a badge to enter Your facilities and comply with Your reasonable physical security and safety policies and procedures while on-site, to the extent they do not violate any applicable law (including privacy laws), place Oracle resources in harm, or require Oracle resources to undergo background checks or other screening (unless set forth in Your order). However, no terms included in any such policies and procedures shall modify the Services, and You shall provide training regarding such policies and procedures as requested.

### **NETWORK ACCESS**

You and Oracle will agree upon the access to Your systems and environments (including cloud tenancies) in order for Oracle to perform the Services. You are responsible for granting, securing, and managing Oracle’s access.

If You and Oracle agree that the Services will be performed remotely, You shall provide and be responsible for maintaining remote access to Your systems and environments (including cloud tenancies) to enable Oracle to perform such Services, using: an Oracle-defined virtual private network; Oracle FastConnect, Oracle Advanced Support Gateway/Portal, or similar Oracle technology; or the Oracle Web Conference or other agreed-upon, third-party web conferencing application (collectively, “remote access tools”).

Oracle is not responsible for any network connections or related problems, or for Your failure to provide and maintain remote access to Your systems and environments.

### **THIRD-PARTY COLLABORATION TOOLS**

If You and Oracle agree, Oracle will provide You with access to third-party tools (e.g., Confluence, Wrike, or Jira) to promote collaboration related to the Services (each, a “collaboration tool”). Upon such access, You agree to:



- Only use a collaboration tool in connection with the Services, and cease use upon the end of the Services or written notice by Oracle, whichever is earlier.
- Promptly notify Oracle when You authorize an individual to use a collaboration tool and when You revoke such authorization due to reassignment, resignation, or termination.
- Do not store source code or product, security, financial, personal, or production data in a collaboration tool.
- Comply with the terms of service for a collaboration tool; specifically, for Wrike at <https://www.wrike.com/security/terms/>; and for Atlassian at <https://www.atlassian.com/legal/atlassian-customer-agreement>.

A collaboration tool is offered on an “as is” and “as available” basis without any warranty, express or implied, or indemnity or liability.

#### **YOUR COOPERATION**

Oracle’s ability to perform the Services depends upon You providing the cooperation listed below and in Your order and as agreed upon during the Services (collectively, “cooperation”):

1. For Services related to Oracle Cloud Services, obtain and maintain the Oracle Cloud Services under separate contract prior to and during the Services.
2. For all other Services: (a) obtain licenses for all applicable Products under separate contract prior to the commencement of the Services; (b) maintain the properly configured hardware/operating system platform to support the Services; and (c) maintain annual technical support for all such Products with access to software patches and updates made available by Oracle under separate contract during the Services.
3. Provide information, data, and documentation agreed upon for the Services.
4. Allocate agreed-upon functional, technical, and business resources, including from Your third parties, with the skills and knowledge to support the performance of the Services.
5. Provide the rights for Oracle to use, on Your behalf, any agreed-upon third-party products that are part of Your system or used to perform the Services.
6. Provide notices and obtain consents agreed upon for Oracle to perform the Services.

If You fail to provide reasonable cooperation, Oracle will not be responsible for any resulting deficiency in performing the Services.

#### **PRIVACY AND SECURITY**

In performing the Services, Oracle will comply with the following documents (which are incorporated herein):

- Oracle Services Privacy Policy, available at <http://www.oracle.com/legal/privacy/services-privacy-policy.html>.
- Oracle Data Processing Agreement for Oracle Services, available at <https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing>.
- Oracle Corporate Security Practices (“Security Practices”), available at <https://www.oracle.com/assets/corporate-security-practices-4490843.pdf>.

The Security Practices cover the management of security for Oracle’s internal operations and the development and delivery of Oracle products and services. These Security Practices apply to all Oracle personnel, including employees and subcontractors, and cover a wide array of topics, such as organizational security, information security, asset management, access control, and security awareness.

### **SUBCONTRACTORS**

Oracle may use subcontractors to support its performance of the Services, subject to any applicable terms and conditions in Your Master Agreement or order; provided that Oracle is responsible for its subcontractors’ performance to the same extent as its employees’ performance.

### **CHANGE CONTROL PROCESS**

All requests for proposed changes to the Services must be in writing, including those related to changes in scope, deliverables, Your cooperation, project assumptions, or any other aspect of Your order.

Oracle shall not be obligated to perform, and You shall not be obligated to pay for, tasks related to any such changes unless agreed upon in an amendment to Your order.

# Privacy @ Oracle

## Oracle Services Privacy Policy

This Oracle Services Privacy Policy (“Services Privacy Policy”) is organized into three sections:

**I. The first section (Services Personal Information Data Processing Terms)** describes the privacy and security practices that Oracle Corporation and its affiliates (“Oracle”) employ when handling Services Personal Information (as defined below) for the provision of Technical Support, Consulting, Cloud or other services, including those provided via mobile application, (the “Services”) provided to Oracle customers (“You” or “Your”) during the term of Your order for Services. Additional terms may be specified in the relevant privacy and security practices for the Services You have ordered.

### Services Personal Information Data Processing Terms Quick Links

[Purpose of Processing Services Personal Information](#)

[Customer instructions](#)

[Rights of individuals](#)

[Security and confidentiality](#)

[Incident Management and breach notification](#)

[Subprocessors](#)

[Cross-border data transfers](#)

[Audit rights](#)

[Deletion or return of Services Personal Information](#)

[Notifications to customers and users](#)

**Services Personal Information** is personal information that is provided by You, resides on Oracle, customer or third-party systems and environments, and is processed by Oracle on Your behalf in order to perform the Services. Services Personal Information may include, depending on the Services: information concerning family, lifestyle and social circumstances; employment details; financial details; online identifiers such as mobile device IDs and IP addresses, geolocation data, and first party online behavior and interest data. Services Personal Information may relate to Your representatives and end users, such as Your employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

**II. The second section (System Operations Data Processing Terms)** describes the privacy and security practices that apply to personal information that may be incidentally contained in Systems Operation Data that is generated by the interaction of (end-)users of our Services (“Users”) with the Oracle systems, tools and networks used to monitor, safeguard and deliver Services to our customer base.



**Systems Operations Data** may include access, event, diagnostic and other log files, as well as statistical and aggregated information that relates to the use and operation of our Services, and the systems and networks these Services run on.

### Systems Operations Data Processing Terms Quick Links

[Responsibility and purposes for processing personal information](#)

[Security](#)

[Sharing personal information](#)

[User choices](#)

[Cross-border data transfers](#)

[Notifications to customers and users](#)

**III. The third section (Communications and Notifications to Customers and Users)** applies to both Services Personal Information and personal information contained in Systems Operations Data, describes how Oracle handles legally required disclosure requests, and informs You and Users how to communicate with Oracle's Global Data Protection Officer or file a complaint.

### Systems Operations Data Processing Terms Quick Links

[Legal requirements](#)

[Dispute resolution or filing a complaint](#)

[Global Data Protection Officer](#)

The definitions of Services Personal Information and Systems Operations Data do not include Your or User **contact and related information** collected from the use of Oracle websites, or Your or User interactions with us during the contracting process. Oracle's handling of this information is subject to the terms of the [General Oracle Privacy Policy](#).

## I. SERVICES PERSONAL INFORMATION DATA PROCESSING TERMS

Oracle treats all Services Personal Information in accordance with the terms of Sections I and III of this Policy and Your order for Services.

In the event of any conflict between the terms of this Services Privacy Policy and any privacy terms incorporated into Your order for Services, including an Oracle Data Processing Agreement, the relevant privacy terms of Your order for Services shall take precedence.

### 1. Purpose of Processing Services Personal Information



Oracle may process Services Personal Information for the processing activities necessary to perform the Services, including for creating an Oracle services account to access Oracle products and services, for testing and applying new product or system versions, patches, updates and upgrades, and resolving bugs and other issues You have reported to Oracle.

## **2. Customer instructions**

You are the controller of the Services Personal Information processed by Oracle to perform the Services. Oracle will process your Services Personal Information as specified in Your Services order and Your documented additional written instructions to the extent necessary for Oracle to (i) comply with its processor obligations under applicable data protection law or (ii) assist You to comply with Your controller obligations under applicable data protection law relevant to Your use of the Services. Oracle will promptly inform You if, in our reasonable opinion, Your instruction infringes applicable data protection law. You acknowledge and agree that Oracle is not responsible for performing legal research and/or for providing legal advice to You. Additional fees may apply.

## **3. Rights of individuals**

You control access to Your Services Personal Information by Your end users, and Your end users should direct any requests related to their Services Personal Information to You. To the extent such access is not available to You, Oracle will provide reasonable assistance with requests from individuals to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to processing of Services Personal Information on Oracle systems. If Oracle directly receives any requests or inquiries from Your end users that have identified You as the controller, we will promptly pass on such requests to You without responding to the end user.

If you are an end user and you have questions about your choices regarding the disclosure and use of Services Personal Information provided to Oracle, please consult directly with the organization that collected your information from you.

## **4. Security and confidentiality**

Oracle has implemented and will maintain technical and organizational measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Services Personal Information. These measures, which are generally aligned with the ISO/IEC 27001:2013 standard, govern all areas of security applicable to the Services, including physical access, system access, data access, transmission, input, security oversight, and enforcement.

Oracle employees are required to maintain the confidentiality of personal information. Employees' obligations include written confidentiality agreements, regular training on information protection, and compliance with company policies concerning protection of confidential information.

See [additional details](#) regarding the specific security measures that apply to the Services are set out in the security practices for these Services, including regarding data retention and deletion, available for review.

## **5. Incident Management and data breach notification.**

Oracle promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or handling of Services Personal Information.

If Oracle becomes aware and determines that an incident involving Services Personal Information qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Services Personal Information transmitted, stored or otherwise processed on Oracle systems that compromises the security, confidentiality or integrity of such Services Personal Information, Oracle will report such breach to You without undue delay.

As information regarding the breach is collected or otherwise reasonably becomes available to Oracle and to the extent permitted by law, Oracle will provide You with additional relevant information concerning the breach reasonably known or available to Oracle.

## **6. Subprocessors**

To the extent Oracle engages Oracle affiliates and third-party subprocessors to have access to Services Personal Information for the purpose of assisting in the provision of Services, such subprocessors shall be subject to the same level of data protection and security as Oracle under the terms of Your order for Services. Oracle is responsible for its subprocessors' compliance with the terms of Your order for Services.

Oracle maintains lists of Oracle affiliates and subprocessors that may process Services Personal Information. Additional information is available to You via My Oracle Support (<https://support.oracle.com>) Document ID 2121811.1, or other applicable primary support tool provided for the Services.

## **7. Cross-border data transfers**

Oracle is a global corporation with operations in over 80 countries and Services Personal Information may be processed globally as necessary in accordance with this policy and other relevant privacy terms specified applicable to Your Services. If Services Personal Information is transferred to an Oracle recipient in a country that does not provide an adequate level of protection for personal information, Oracle will take adequate measures designed to protect the Services Personal Information, such as ensuring that such transfers are subject to the terms of the EU Standard Contractual Clauses or other adequate transfer mechanism as required under relevant data protection laws.

In the event the Services agreement between You and Oracle references the [Oracle Data Processing Agreement for Oracle Services](#) ("DPA"), further details on the relevant data transfer

mechanism that applies to Your order for Oracle services are available in the DPA. In particular, for Services Personal Information transferred from the European Economic Area (EEA) or Switzerland, such transfers are subject to Oracle's Binding Corporate Rules for Processors (BCR-P) or the terms of the EU Standard Contractual Clauses. For Services Personal Information transferred from the United Kingdom (UK), such transfers are subject to the UK Addendum or other appropriate transfer mechanism.

Oracle also complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) (collectively, the "DPF") as set forth by the U.S. Department of Commerce, regarding the collection, use, and retention of Services Personal Information when You and Oracle have agreed by contract that transfers of such information from the EEA, United Kingdom (and Gibraltar), or Switzerland will be transferred and processed pursuant to the applicable DPF for the relevant Services. Oracle will then be responsible for ensuring that third parties acting as a subprocessor on our behalf do the same. Oracle shall remain liable under the DPF Principles if its subprocessor processes Services Personal Information in a manner inconsistent with the DPF Principles, unless Oracle proves that it is not responsible for the event giving rise to the damage.

Oracle has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with regard to Services Personal Information (as described above) that is transferred from the European Union, the United Kingdom (and Gibraltar), and/or Switzerland to the United States when specified in a relevant contract. If there is any conflict between the terms in this Services Privacy Policy and the DPF Principles, the DPF Principles shall govern. To learn more about the DPF program, and to view Oracle's certification, please visit [Data Privacy Framework website](#). Please see the [Data Privacy Framework website](#) or refer to [this list](#) of U.S. entities covered under Oracle's DPF self-certification. With respect to Services Personal Information received or transferred pursuant to the DPF, the Federal Trade Commission has jurisdiction over Oracle's compliance with the DPF.

## **8. Audit rights**

To the extent provided in your order for Services, You may at Your sole expense audit Oracle's compliance with the terms of this Services Privacy Policy by sending Oracle a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. You and Oracle will work cooperatively to agree on a final audit plan.

The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to Oracle's on-site policies and regulations, and may not unreasonably interfere with business activities. If You would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle. Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is classified as confidential information under the terms of Your agreement with Oracle.

Oracle will contribute to such audits by providing You with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services. If the requested audit scope is addressed in a SOC 1 or SOC 2, ISO,



NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report. Additional audit terms may be included in Your order for Services.

## **9. Deletion or return of Services Personal Information**

Except as otherwise specified in an order for services or required by law, upon termination of services, Oracle will return or delete any remaining copies of Your production customer data, including any Services Personal Information, located on Oracle systems or Services environments. Additional information on data deletion functionality is provided in the applicable Services descriptions.

## **II. SYSTEMS OPERATIONS DATA PROCESSING TERMS**

### **1. Responsibility and purposes for processing personal information**

Oracle Corporation and its affiliated entities are responsible for processing personal information that may be incidentally contained in Systems Operations Data in accordance with Sections II and III of this Policy. See the list of [Oracle entities](#). Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country. We may collect or generate Systems Operations Data for the following business purposes:

- a) to help keep our Services secure, including for security monitoring and identity management;
- b) to investigate and prevent potential fraud or illegal activities involving our systems and networks, including to prevent cyber-attacks and to detect bots;
- c) to administer our back-up disaster recovery plans and policies;
- d) to confirm compliance with licensing and other terms of use (license compliance monitoring);
- e) for research and development purposes, including to analyze, develop, improve and optimize our Services;
- f) to comply with applicable laws and regulations and to operate our business, including to comply with legally mandated reporting, disclosure or other legal process requests, for mergers and acquisitions, finance and accounting, archiving and insurance purposes, legal and business consulting and in the context of dispute resolution.

Where relevant, our legal basis for processing Your personal information is as follows:

- Oracle will process Systems Operations Data as may be necessary to help keep our Services secure; to investigate and prevent potential fraud or illegal activities involving our systems and networks; to administer our back-up disaster recovery



plans and policies; and to confirm compliance with licensing and other terms of use.

- Oracle will process Systems Operations Data as may be necessary for internal research for technological development and demonstration and to improve, upgrade, or enhance Oracle products and services based on our legitimate interests when such processing has a limited privacy impact on the individual.
- Oracle may also process Systems Operations Data as necessary for compliance with our legal obligations and for required business operations as noted above.

## **2. Sharing personal information**

Personal information contained in Systems Operations Data may be shared throughout Oracle's global organization for Oracle's business purposes. A list of Oracle entities is available as indicated above.

We may also share such personal information with the following third parties:

- third-party service providers (for example IT service providers, lawyers and auditors) in order for those service providers to perform business functions on behalf of Oracle;
- relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings);
- as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

When third parties are given access to personal information contained in Systems Operations Data, we will take the appropriate contractual, technical and organizational measures to ensure, for example, that personal information is only processed to the extent that such processing is necessary, consistent with this Privacy Policy and in accordance with applicable law. Oracle does not share or sell Systems Operations Data subject to this Privacy Policy with third parties for any commercial purposes.

## **3. Cross-border data transfers**

If personal information contained in Systems Operations Data is transferred to an Oracle recipient in a country that does not provide an adequate level of protection for personal information, Oracle will take measures designed to adequately protect information about Users, such as ensuring that such transfers are subject to the terms of the EU Standard Contractual Clauses or other adequate transfer mechanism as required under relevant data protection laws.

## 4. Security

Oracle has implemented appropriate technical, physical and organizational measures in accordance with the Oracle Corporate Security Practices designed to protect personal information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

## 5. Individual rights

To the extent personal information about You is contained in Systems Operations Data, You may request to access, correct, update or delete personal information contained in Systems Operations Data in certain cases, or otherwise exercise Your choices with regard to Your personal information by filling out an [inquiry form](#). We will respond to your request consistent with applicable law.

If are a California resident, under the California Consumer Privacy Act (CCPA), as amended, You may request that Oracle:

1. Discloses to you the following information:
  - the categories and specific pieces of personal information we collected about You and the categories of personal information we sold, if applicable;
  - the categories of sources from which we collected such personal information;
  - the business or commercial purpose for collecting or selling personal information; and
  - the categories of third parties to whom we sold or otherwise disclosed personal information, if applicable.
2. deletes personal information we collected about You or corrects inaccurate personal information about You, unless retained solely for legal and compliance purposes and as otherwise set out in the CCPA
3. fulfils your request to opt-out of any future sale of personal information about You, if applicable.

If You are an authorized agent making an access or deletion request on behalf of a California resident, please reach out to us via the [inquiry form](#) and indicate that You are an authorized agent. We will provide You with instructions on how to submit a request as an authorized agent on behalf of a California resident.

If you submit a request, please be specific as to what right you are asserting (e.g., access, correction, etc.) and which specific pieces of personal information are in scope of your request. In some cases, in order to comply with applicable law or a legal obligation, Oracle may deny your request or may seek more information from you in order to respond to your request.

If You are a California resident, you may obtain information about exercising your rights, as described above, by contacting us at 1-800-633-0748. For information on the CCPA requests

Oracle received, complied with, or denied for the previous calendar year, please visit Oracle's Annual Consumer Privacy Reporting page, available [here](#).

### **III. COMMUNICATIONS AND NOTIFICATIONS TO CUSTOMERS AND USERS**

#### **1. Legal requirements.**

Oracle may be required to provide access to Services Personal Information and to personal information contained in Systems Operations Data as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect Your or a User's safety or the safety of others, investigate fraud, or respond to government requests, including public and government authorities outside Your or a User's country of residence, for national security and/or law enforcement purposes.

Oracle will promptly inform You of requests to provide access to Services Personal Information, unless otherwise required by law.

#### **2. Global Data Protection Officer**

Oracle has appointed a Global Data Protection Officer who is also Oracle's Chief Privacy Officer. If You or a User believe that personal information has been used in a way that is not consistent with this Privacy Policy, or if You or a User have further questions, comments or suggestions related to Oracle's handling of Services Personal Information or personal information contained in Systems Operations Data, please contact the Data Protection Officer by filling out an [inquiry form](#).

Written inquiries to the Global Data Protection Officer may be addressed to:

Oracle Corporation  
Global Data Protection Officer  
Willis Tower  
233 South Wacker Drive  
45th Floor  
Chicago, IL 60606  
U.S.A.

For personal information collected INSIDE the EU/EEA, You may contact Oracle's external EU Data Protection Officer by filling out the [inquiry form](#) and selecting "Other Privacy Inquiry - Contact our DPO" in our drop down box or by written inquiry to.

Robert Niedermeier  
Hauptstraße 4  
D-85579 Neubiberg / München  
Germany

For personal information collected INSIDE Brazil, written inquiries to the Brazilian Data Protection Officer may be addressed to:

Alexandre Sarte  
Rua Dr. Jose Aureo Bustamante, 455  
Vila São Francisco  
São Paulo, BR

### **3. Filing a complaint**

If You or a User have any complaints regarding our compliance with our privacy and security practices, please contact us via our [inquiry form](#). We will investigate and attempt to resolve any complaints and disputes regarding our privacy practices. Users also have the right to file a complaint with a [competent data protection authority](#) if they are a resident of a European Union member state.

We commit to refer unresolved complaints concerning our handling of Services Personal Information received in reliance on the DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit [TRUSTe](#) for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

Under certain conditions, specified on the DPF website, Users may invoke binding arbitration after other dispute resolution procedures have been exhausted.

### **4. Changes to this Services Privacy Policy**

This Privacy Policy was last updated on February 21, 2024. However, the Services Privacy Policy can change over time, for example to comply with legal requirements or to meet changing business needs. The most up-to-date version can be found on this [website](#). In cases of material changes, we will also inform you in another appropriate way (for example via a pop-up notice or statement of changes on our website) prior to the changes becoming effective.

Previous versions: [12/23/22](#) | [8/5/22](#) | [4/9/21](#) | [1/19/21](#) | [10/20/20](#) | [3/7/19](#) | [2/14/19](#)

---



---

# Data Processing Agreement for Oracle Services

## ("Data Processing Agreement")

Version January 1, 2023

### 1. Scope and Applicability

This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

### 2. Responsibility for Processing of Personal Information and Description of Processing Activities

2.1 You are a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Oracle will Process Personal Information during the term of the Services Agreement solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In particular and depending on the Services, Oracle may Process Personal Information for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.4 As part of the provision of the Services and depending on the Services, Oracle may Process Personal Information about Your Individuals, including Your end users, employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Personal Information about Your Individuals may include, but is not limited to, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; geolocation data; IP addresses and online behavior and interest data.

2.6 Unless otherwise specified in the Services Agreement, You may not provide Oracle with any data that imposes specific data security or data protection obligations on Oracle in addition to or different from those

specified in the Data Processing Agreement or Services Agreement (e.g. certain regulated health or payment card information). If available for the Services, You may purchase additional services from Oracle (e.g., Oracle Payment Card Industry Compliance Services) designed to address specific data security or data protection requirements applicable to sensitive or special data You seek to include in Your Content. You remain responsible for compliance with Your specific regulatory, legal or industry data security obligations which may apply to such data.

2.7 Additional or more specific descriptions of Processing activities may be included in the Services Agreement.

2.8 Oracle is a Service Provider in respect to Personal Information processed in performance of the Services. Oracle will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Services Agreement, including for any Commercial Purpose, or (ii) outside of the direct business relationship between Oracle and You; or (c) combine Personal Information received from or on behalf of You with Personal Information received from or on behalf of any third party, or collected from Oracle's own interaction with Individuals, except to perform a Business Purpose that is permitted by the CCPA and the Services Agreement. Oracle will notify You of its use of Oracle Affiliates and Third Party Subprocessors in accordance with Section 5 of this Data Processing Agreement; and ensure Oracle Affiliates and Third Party Subprocessors are subject to applicable written agreements per Section 5 of this Data Processing Agreement. The parties acknowledge that the Personal Information You disclose to Oracle is provided only for the limited and specified Business Purposes set forth in the Services Agreement. Oracle shall provide the same level of protection to Personal Information as required by the CCPA and as more fully set out in the Services Agreement. You may take such reasonable steps as may be necessary (a) to remediate Oracle's unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this Data Processing Agreement by exercising Your rights under Section 8 of this Data Processing Agreement. Oracle shall notify You if it makes a determination that it is not able to meet its obligations under the CCPA in connection with its provision of the Services.

### **3. Your Instructions**

3.1 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

3.2 Oracle will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. Oracle will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. Oracle is not responsible for providing legal advice to You.

3.3 To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

#### **4. Privacy Inquiries and Requests from Individuals**

4.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by Oracle under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address the request. Additional information on how to access the Services to address privacy requests or inquiries from Individuals is available in the applicable Oracle Product or Service Feature Guidance documentation available on My Oracle Support (or other applicable primary support tool or support contact provided for the Services).

4.2 To the extent access to the Services is not available to You or otherwise not responsive to the request or inquiry, You can submit a "service request" via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to Oracle on how to assist You with such request.

4.3 If Oracle directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

#### **5. Oracle Affiliates and Third Party Subprocessors**

5.1 You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

5.2 To the extent Oracle engages such Third Party Subprocessors and/or Oracle Affiliates, it requires that such entities are subject to the same level of data protection and security as Oracle under the terms of this Data Processing Agreement and Applicable Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Information. Oracle remains responsible for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of the Services Agreement.

5.3 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via [My Oracle Support](#), Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the [NetSuite Support Portal](#) or Your Oracle project manager). To receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, You can (i) sign up per the instructions on My Oracle Support, Document ID 2288528.1; or (ii) Oracle will provide you notice of intended changes where a sign up mechanism is not available. For ACS and Consulting Services, any additional Third Party Subprocessors that Oracle intends to use will be listed in Your order for ACS or Consulting Services, or in a subsequent "Oracle Subprocessor Notice", which Oracle will send to you by e-mail as necessary.

5.4 Within thirty (30) calendar days of Oracle providing such notice to You under Section 5.3 above, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services by submitting a "service request" via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. You and Oracle



will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 5.4 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

## **6. Cross-border data transfers**

6.1 For Cloud Services, Personal Information will be stored in the data center region specified in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services.

6.2 Without prejudice to Section 6.1 above, Oracle may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes.

6.3 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable European Data Protection Law to countries outside Europe not covered by an adequacy decision, such transfers are subject to (i) Oracle's Binding Corporate Rules for Processors or BCR-p (also referred to as the Oracle Processor Code) and (ii) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021.

The most current version of Oracle's Binding Corporate Rules for Processors (Oracle Processor Code) is available on <https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing>, and is incorporated by reference into the Services Agreement and this Data Processing Agreement. Oracle has obtained EEA authorization for its Binding Corporate Rules for Processors (Processor Code) and will maintain such authorization for the duration of the Services Agreement. Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with Oracle's Binding Corporate Rules for Processors (Oracle Processor Code), the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021, this Data Processing Agreement and the Services Agreement.

6.4 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable UK Data Protection Law, to countries outside the United Kingdom not covered by an Adequacy Decision by the UK ICO, such transfers are subject to (i) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021 as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (the "IDTA"), which are incorporated herein by reference; and (ii) when approved by the UK ICO, the approved UK Binding Corporate Rules for Processors, in the form that will be approved by the UK ICO for use in the UK and will be published on Oracle's public websites. The IDTA will be read in conjunction with the Services Agreement and the Data Processing Agreement.

6.5 The parties will review any supplemental measures, which may be required based on applicable Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of

protection. The parties will work together in good faith to find a mutually acceptable resolution to address such supplementary measures, including but not limited to reviewing technical documentation for the Services, and discussing additional available technical safeguards and security services.

6.6 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under other Applicable Data Protection Laws globally, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

## 7. Security and Confidentiality

7.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services:

- For **all Services**: Oracle's Corporate Security Practices, available at <https://www.oracle.com/corporate/security-practices/>;
- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at <http://www.oracle.com/us/corporate/contracts/cloud-services/index.html>;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: <http://www.netsuite.com/portal/resource/terms-of-service.shtml>;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: <https://www.oracle.com/support/policies.html>;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: <http://www.oracle.com/us/corporate/contracts/consulting-services/index.html>.

7.2 All Oracle and Oracle Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

## 8. Audit Rights and Assistance with Data Protection Impact Assessments

8.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year, including inspections of the applicable Services data center facility that hosts Personal Information. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

8.2 If You engage a third party auditor, the third party must be mutually agreed to by You and Oracle



(except if such third party is a Regulator). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory or legal confidentiality obligation.

8.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

8.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

8.5 Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

8.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

8.7 Without prejudice to the rights granted in Section 8.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

8.8 You may also request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations.

8.9 Oracle provides You with information and assistance reasonably necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and Oracle Product/Service privacy & security functionality guides for the Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Services, such as the [NetSuite Support Portal](#), or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to You.

## **9. Incident Management and Breach Notification**

9.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Your Content (as such term is defined in the Services Agreement) transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if an



Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

9.2 Oracle will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

## **10. Return and Deletion of Personal Information**

10.1 Upon termination of the Services, Oracle will promptly return, including by providing available data retrieval functionality, and subsequently delete any remaining copies of Personal Information on Oracle systems or Services environments, except as otherwise stated in the Services Agreement.

10.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by Oracle as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

## **11. Legal Requirements**

11.1 Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

11.2 Oracle will promptly inform You of requests to provide access to Personal Information and use reasonable efforts to redirect the authority that made the request to You, unless otherwise required by law.

11.3 To the extent Oracle is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on Oracle, including whether the request is consistent with Applicable Data Protection Law. Any request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law.

## **12. Data Protection Officer**

12.1 Oracle has appointed a Chief Privacy Officer and a local Data Protection Officer in certain countries. Further details on how to contact Oracle's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available at <https://www.oracle.com/legal/privacy/index.html>.

12.2 If You have appointed a Data Protection Officer, You may request Oracle to include the contact details of Your Data Protection Officer in the relevant Services order.

### 13. Definitions

**"Applicable Data Protection Law"** means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended ("CCPA") and other US State laws.

**"Applicable European Data Protection Law"** means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.

**"Applicable UK Data Protection Law"** means (i) the UK GDPR, meaning the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020; and (ii) the UK Data Protection Act 2018, as amended.

**"Europe"** means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.

**"Individual"** shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

**"Information Breach"** means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Content transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of Your Content.

**"Process/Processing", "Controller", "Processor" and "Binding Corporate Rules"** (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

**"Service Provider", "Sell", "Share", "Business Purpose", and "Commercial Purpose"** have the meaning set forth under the CCPA.

**"Oracle Affiliate(s)"** means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in this Data Processing Agreement.

**"Oracle Intra-Company Data Transfer and Mandate Agreement"** means the Oracle Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

**"Oracle Binding Corporate Rules for Processors" or "Oracle Processor Code"** means the EU or UK Oracle's Privacy Code for Processing Personal Information of Customer Individuals, as the case may be.

**"Oracle"** means the Oracle Affiliate that has executed the Services Agreement.

**"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.

“**Regulator**” shall have the same meaning as the term “supervisory authority”, “data protection authority” or the equivalent term under Applicable Data Protection Law.

“**Services**” or the equivalent terms “Service Offerings” or “services” means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

“**Services Agreement**” means (i) the applicable order for the Services you have purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications.

“**Third Party Subprocessor**” means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in this Data Processing Agreement.

“**You**” means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.



ORACLE

# Oracle Corporate Security Practices

---

April 2024 | Version 3.3  
Copyright © 2024, Oracle and/or its affiliates  
Oracle – Public



## INTRODUCTION

Oracle's mission is to help people see data in new ways, discover insights and unlock endless possibilities.

Oracle's security practices reflect the various ways Oracle engages with its customers:

- Oracle Corporate Security programs, policies and recommendations guide the IT teams managing Oracle's corporate network and systems as well as guiding the operational, cloud and services Lines of Business.
- In this document, "customer data" means any data stored in a customer's computer system (data accessed by or provided to Oracle while performing services for a customer) or data in a customer's cloud tenancy.
- Third parties provided access to customer data by Oracle ("subprocessors") are required to contractually commit to materially equivalent security practices.

Oracle continually works to strengthen and improve the security controls and practices for internal operations and services offered to customers. These practices are subject to change at Oracle's discretion.

Companies that Oracle acquires are required to align with these security practices as part of the integration process. This duration and outcome of each aspect of the integration process relies on the size, complexity, contractual commitments and regulatory requirements applicable to the acquired company's products, services, personnel and operations.

Oracle's Cloud, Support, and Services lines of business have developed statements of security practices that apply to the respective service offerings. These are published and incorporated into applicable orders.

The purpose of this paper is to summarize key Oracle's security practices and programs. This paper does not exhaustively describe all security practices and programs which may be applicable and relevant to individual Lines of Business, products or services.

# TABLE OF CONTENTS

<b>Introduction</b>	<b>1</b>
<b>Oracle Corporate Security</b>	<b>3</b>
<b>Organizational Security</b>	<b>3</b>
Oracle Security Oversight Committee	3
Corporate Security Organizations	3
Global Information Security	3
Global Product Security	3
Global Physical Security	3
Corporate Security Architecture	4
Global Trade Compliance	4
Line of Business Security Organizations	4
Oracle Information Technology Organizations	4
Independent Review of Information Security	4
<b>Privacy</b>	<b>4</b>
<b>Customer Data Protection</b>	<b>5</b>
<b>Asset Classification and Control</b>	<b>5</b>
Responsibility, Inventory, and Ownership of Assets	5
Asset Classification and Control	5
<b>Human Resources Security</b>	<b>5</b>
Employee Screening	5
Confidentiality Agreements	5
Security Awareness Education and Training	6
<b>Physical Security</b>	<b>6</b>
<b>Operations Management</b>	<b>6</b>
Protection Against Malicious Code	6
Monitoring and Protection of Audit Log Information	6
Network Controls	7
<b>Access Control</b>	<b>7</b>
User Access Management	7
Privilege Management	7
Password Management	8
Periodic Review of Access Rights	8
<b>Information Systems Development, and Maintenance</b>	<b>8</b>
Technical Vulnerability Management	8
<b>Information Security Incident Response</b>	<b>8</b>
Security Incident Policy and Operations	8
Notifications	9
<b>Oracle Software Security Assurance</b>	<b>9</b>
Coding Standards & Security Training	9
Security Analysis & Testing	10
Security Fixing Policies	10
Applicability of Critical Patch Updates and Security Alerts to Oracle Cloud Environments	10
Source Code Protection	10
External Security Evaluations	11
<b>Resilience Management</b>	<b>11</b>
<b>Revision History</b>	<b>12</b>



## ORACLE CORPORATE SECURITY

Oracle's Corporate Security Programs are designed to protect both Oracle and customer data, such as:

- Mission-critical systems that customers rely upon for cloud, technical support and other services
- Oracle source code and other sensitive data against theft and malicious alteration
- Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle's internal IT systems

Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are generally aligned with the ISO/IEC 27002:2022 and ISO/IEC 27001:2022 standards and guide security within Oracle.

Reflecting the recommended practices in security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective and corrective security controls with the objective of protecting information assets.

## ORGANIZATIONAL SECURITY

Oracle's overarching Organizational Security is described in the Oracle security organization policy and the Oracle information security policy.

The Chief Corporate Architect is one of the directors of the Oracle Security Oversight Committee. The Chief Corporate Architect manages the Corporate Security departments which guide security at Oracle. These departments manage the corporate security programs, define corporate security policies, and provide global oversight for Oracle's security policies and requirements.

## Oracle Security Oversight Committee

The Oracle Security Oversight Committee (OSOC) oversees the implementation of Oracle-wide security programs, including security policies and data privacy standards. The OSOC is chaired by Oracle's CEO, General Counsel, and Chief Corporate Architect.

## Corporate Security Organizations

### Global Information Security

Global Information Security (GIS) defines policies for the management of information security across Oracle. GIS provides direction and advice to help Lines of Business (LoBs) protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle.

### Global Product Security


The Global Product Security organization acts as a central resource to help Oracle development teams improve the security of Oracle products. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products.

Under the leadership of Oracle's Chief Security Officer, Global Product Security promotes the use of Oracle Software Security Assurance standards throughout Oracle, acts as a central resource to help development teams improve the security of their products, and handles specialized security functions.

### Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. Oracle's physical security standards and policies have been developed to generally align with several physical security industry initiatives, including the International Organization for Standardization (ISO), United States Customs Trade Partnership Against Terrorism (CTPAT), American





Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, and the Payment Card Industry Security Standards Council. Physical security controls are described later in this document.

## Corporate Security Architecture

The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's information security goals. The corporate security architect works with Global Information Security and Global Product Security, and the Development Security Leads to develop, communicate and implement secure architectures.

Corporate Security Architecture (CSA) manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud and all other lines of business.

## Global Trade Compliance

Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance and enforcement to enable worldwide trade compliant business processes across Oracle in order to uphold and protect Oracle's global trade privileges. GTC manages Oracle's global trade compliance portfolio and is responsible for global trade regulatory interpretation and coordination of policy advocacy, Global Brand Protection, Hardware Compliance Strategy and Market Access programs. Further, GTC reviews and resolves global trade compliance matters; serves as the clearinghouse for all global trade compliance information, including product classification, and is empowered to take actions necessary to ensure Oracle remains compliant with U.S. and applicable local Customs, import, and export laws, regulations and statutes.

## Line of Business Security Organizations

Lines of Business (LoB) have security teams which oversee their products, systems and cloud services managed by that organization. LoBs are required to define technical standards in accordance with Oracle's information security policies, as well as drive compliance to Oracle policies and standards within their organization and cloud service teams. LoBs are also required to comply with Corporate Security program requirements and directions. This paper does not describe LoB's specific security organizations, standards, and programs.

## Oracle Information Technology Organizations

Oracle information technology (IT) and cloud DevOps organizations are responsible for IT security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation and security technical assessment for new infrastructure.

## Independent Review of Information Security

Oracle's Business Assessment & Audit is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business.

## PRIVACY

The Oracle General Privacy Policy addresses information we collect in connection with your use of Oracle websites, mobile applications, and social media pages that link to the General Privacy Policy, your interactions with Oracle during in-person meetings at Oracle facilities or at Oracle events, and in the context of other online or offline sales and marketing activities.

The Services Privacy Policy describes our privacy and security practices that apply when handling (i) services personal information in order to perform Consulting, Technical Support, Cloud and other services on behalf of Oracle customers; and (ii) personal information contained in systems operation data generated by the interaction of (end-)users of these services with Oracle systems and networks. Oracle Advertising Privacy Policy (also referred to as the 'Privacy Policy' or the 'Oracle Data Cloud Privacy Policy') informs consumers on the collection, use, sharing, and selling (collectively referred to as 'processing') of your personal information in connection with Oracle's provision of Oracle Advertising services designed to help Oracle's customers' and partners' online and offline marketing activities ('Oracle Advertising'). This policy also explains your privacy rights in relation to these processing activities.



## CUSTOMER DATA PROTECTION

Oracle's media sanitation and disposal policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required against unauthorized retrieval and data reconstruction. Electronic storage media include laptops, hard drives, storage devices and removable media.

## ASSET CLASSIFICATION AND CONTROL

### Responsibility, Inventory, and Ownership of Assets

Oracle's formal information protection policy provides guidelines for all Oracle information classification and minimum handling requirements for each classification.

Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's information systems asset inventory policy requires that Lines of Business (LoBs) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services.

### Asset Classification and Control

Oracle categorizes information into four classes—Public, Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data:

- "Public" information is not sensitive, and there is no need with it remaining confidential to Oracle.
- "Oracle Internal" information must remain confidential to Oracle.
- "Oracle Restricted" and "Oracle Highly Restricted" information must remain confidential to Oracle and access within Oracle must be restricted on a "need to know" basis, with additional handling requirements for "Oracle Highly Restricted" information.

Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Retention of customer data in cloud services is controlled by the customer and is subject to terms in their contract.

Customer data is classified under one of Oracle's top two categories of confidential information for the purpose of placing limits on access, distribution and handling of such data. Oracle keeps the information confidential in accordance with the terms of customer's order.

## HUMAN RESOURCES SECURITY

Oracle places a strong emphasis on personnel security. The company maintains ongoing initiatives intended to help minimize risks associated with human error, theft, fraud and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.

Employees who fail to comply with Oracle policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

### Employee Screening

In the United States, Oracle currently uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations and local Oracle policy.

### Confidentiality Agreements

Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms



of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.

## Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters and security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers privacy principles and data handling practices required by company policy.

## PHYSICAL SECURITY

Oracle Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.

Oracle currently has implemented the following protocols in Oracle facilities:

- Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.
- Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle.
- Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination.
- Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.
- Mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of physical security events.
- Centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as per Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws.

## OPERATIONS MANAGEMENT

### Protection Against Malicious Code

Oracle policy requires the use of antivirus protection and firewall software on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.


The Oracle information technology organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. They are responsible for:

- notifying internal Oracle system users of both any credible virus threats and when security updates are available
- providing automation to manage and verify antivirus configuration

Employees are prohibited from altering, disabling or removing antivirus software and the security update service from any computer. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.

### Monitoring and Protection of Audit Log Information

Oracle logs certain security-related activities on operating systems, applications, databases and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages and system errors. Oracle



implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events and/or logs being overwritten.

Oracle reviews logs for security event investigation and forensic purposes. Identified anomalous activities feed into security event management processes. Access to security logs is provided on the basis of need-to-know and least privilege. Where available for cloud services, log files are protected by strong cryptography and other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

## Network Controls

Oracle has implemented and maintains strong network controls for the protection and control of both Oracle and customer data during its transmission. Oracle's network security policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated.

For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measures defined by Global Physical Security (GPS).

Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use approved virtual private networks (VPNs). Corporate systems available outside the corporate network are protected by alternative security controls such as multifactor authentication.

Oracle's network security policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.

Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle's third-party network access policy.

## ACCESS CONTROL

Access control refers to the policies, procedures and tools that govern access to and use of resources. Examples of resources include a physical server, file, application, data in a database and network device.

- Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.
- Default-deny is a network-oriented configuration approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.

Oracle's logical access control policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability and auditing functionality. This policy does not apply to customer end user accounts for Oracle cloud services.

## User Access Management

Oracle user access is provisioned through an account provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, database administrators, system administrators, and network engineers.

## Privilege Management

Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval and review of access are based on the following principles:

- Need to know: Does the user require this access for his job function?
- Segregation of duties: Will the access result in a conflict of interest?



- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

## Password Management

The use of passwords is addressed in the Oracle password policy. Oracle has strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt.

Employees must keep their passwords confidential and secured at all times and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Oracle system or applications passwords for non-Oracle applications or systems.

## Periodic Review of Access Rights

Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony and physical access.

# INFORMATION SYSTEMS DEVELOPMENT, AND MAINTENANCE

## Technical Vulnerability Management

Oracle has formal practices designed to identify, analyze, and remediate the technical security vulnerabilities that may affect our enterprise systems and your Oracle Cloud environment.

The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internal and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments.

Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud is to remediate these issues according to their severity and the potential impact. The Common Vulnerability Scoring System (CVSS) is one of the criteria used in assessing the relative severity of vulnerabilities and their potential impact. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system.

Oracle aims to complete all cloud remediation activities, including testing, implementation, and reboot (if required) within planned maintenance windows. Emergency maintenance will be performed as described in the Oracle Cloud Hosting and Delivery Policies and applicable Pillar documentation.

Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud.

Customers and security researchers can report suspected security vulnerabilities: [How to Report Security Vulnerabilities to Oracle](#) or by submitting a [Service Request in their designated support system](#).

# INFORMATION SECURITY INCIDENT RESPONSE

A security incident is a security event that Oracle, per its incident response process, has determined results in the actual or potential loss of confidentiality, integrity, or availability of Oracle managed assets (systems and data).

Oracle will respond to information security events when Oracle suspects unauthorized access to Oracle-managed assets. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logging.

## Security Incident Policy and Operations

Oracle's Security Incident Management Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction



for security event and incident preparation, detection, investigation, resolution and forensic evidence handling across Oracle's Lines of Business (LoB). This policy does not apply to availability issues (outages) or to physical security events.

Global Information Security further defines roles and responsibilities for the incident response teams within the LoBs. All LoBs must comply with Global Information Security guidance for managing information security events and implementing timely corrective actions.

Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. LoB incident response teams, as required by the Security Incident Management Policy, conduct post-event analysis to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Oracle can support legally admissible forensic data collection when necessary.

## Notifications

If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the [Data Processing Agreement for Oracle Services](#). Information about malicious attempts, suspected incidents and incident history are not shared externally.

## ORACLE SOFTWARE SECURITY ASSURANCE

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing and maintenance of its products, whether they are used on-premises by customers or delivered through Oracle cloud services.

Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

- **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the cloud.
- **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups and the use of automated analysis and testing tools.
- **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

## Coding Standards & Security Training

Developing secure software requires consistently applied methodologies across the organization; methodologies that conform to stated policies, objectives, and principles. Oracle's objective is to produce secure code. To that end, Oracle requires that all of development abide by secure coding principles that are documented and maintained to remain relevant. Developers must be familiar with these standards and apply them when designing and building Oracle products.

Oracle Secure Coding Standards and related guidance have evolved and expanded over time to encompass emerging technologies such as Artificial Intelligence and Machine Learning (AI/ML) and address the most common issues affecting Oracle code, new threats as they are discovered, and new customer use cases for Oracle technology.

All Oracle staff are required to take security training. Technical development staff, up to and including vice presidents, who are involved in building, maintaining, customizing or testing product code are required to take an OSSA awareness course.

Additionally, Oracle adapted its secure coding principles and created training material for use by its consulting and services organizations when they are engaged in producing code on behalf of customers.

## Security Analysis & Testing

Oracle requires that security testing be performed for its on-premises and cloud products. Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to support comprehensive security testing coverage of Oracle products.

Functional security testing is typically executed by regular product Quality Assurance (QA) teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process.

Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis:

- Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written.
- Dynamic analysis activity takes place during latter phases of product development: at the very least, the product or component should be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing at Oracle. Automatic tools employ fuzzing technique to test network-accessible product interfaces and protocols, while manual tools require making the modifications by hand.

Oracle will not provide customers sensitive security assurance artifacts (including but not limited to static code analysis reports). Oracle will not submit its product to third-party static code assessments. For more information, see MOS Article: General Instructions for Submitting Security Questionnaires to Oracle (Doc ID 2337651.1).

## Security Fixing Policies

The Critical Patch Update (CPU) is the primary mechanism for the backport of security bug fixes for all Oracle on-premises products. Critical Patch Updates are available to customers with valid support contracts. Critical Patch Updates are released quarterly on the third Tuesday of January, April, July, and October. Oracle retains the ability to issue out of schedule patches or workaround instructions in case of particularly critical vulnerabilities and/or when active exploits are reported in the wild. This program is known as the Security Alert program.

Vulnerabilities are remediated by Oracle in order of the risk they pose to users. This process is designed to patch the security defects with the greatest associated risk first in the Critical Patch Update, resulting in optimizing the security posture of all Oracle customers.

A standardized CPU schedule helps organizations plan their security maintenance windows. The CPU schedule is designed to avoid typical blackout dates during which customers cannot typically alter their production environments.

As much as possible, Oracle tries to make Critical Patch Updates cumulative; that is, each Critical Patch Update contains the security fixes from all previous Critical Patch Updates. This provides customers the ability to catch up quickly to the current security release level, since the application of the latest cumulative CPU resolves all previously addressed vulnerabilities.

## Applicability of Critical Patch Updates and Security Alerts to Oracle Cloud Environments


The Oracle Cloud operations and security teams regularly evaluate Oracle's Critical Patch Updates and Security Alerts as well as relevant third-party security updates as they become available and apply the relevant patches in accordance with applicable change management processes.

## Source Code Protection

Oracle maintains strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories.

Oracle Software Security Assurance policies and practices are designed to prevent the introduction of security vulnerabilities in Oracle-developed code. Additionally, Oracle maintains strong controls over the technical description of security vulnerabilities in Oracle code. Oracle's Security Vulnerability Information Protection Policy defines the classification and





handling of information related to product security vulnerabilities and requires that information concerning security bugs be recorded in a tightly controlled database.

Oracle's policies prohibit the introduction of backdoors into its products. Backdoors are deliberately (and maliciously) introduced code intended to bypass the security controls of the application in which it is embedded. Backdoors do not include:

- Unintentional defects in software that could lead to a weakening of security controls (security bugs)
- Undocumented functionality designed to be generally inaccessible by customers but serves a valid business or technical purpose (diagnostics and troubleshooting utilities)

Oracle assesses third-party software and hardware to avoid the use of products:

- With known vulnerabilities
- Developed with poor security assurance
- That may potentially include backdoors or other malicious components

## External Security Evaluations

Oracle submits certain products for external security evaluations. These evaluations involve rigorous testing by independently accredited organizations ("labs") with further oversight and certification completed by government bodies. Independent verification helps provide additional assurance to Oracle customers with regards to the security posture of the validated products. Organizations in many industries have business and compliance requirements that imply the use of validated products. Such evaluations include Common Criteria and FIPS 140.

## RESILIENCE MANAGEMENT

Oracle's risk management resiliency policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation and executive approvals for critical business operations.

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations.

The RMRP approach is comprised of several subprograms: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.

Each of these subprograms is a uniquely diverse discipline. By consolidating emergency response, crisis management, business continuity and disaster recovery, they can become a robust collaborative and communicative system.





## REVISION HISTORY

Version 3.3	04 Apr 2024	Updated introduction, information security incident response and Oracle Software Security Assurance sections
Version 3.2	12 Sep 2023	Clarified physical security and technical vulnerability management controls
Version 3.1	20 Jan 2023	Expanded Oracle Software Security Assurance (OSSA) section and updated the order of sections.
Version 3.0	30 Sep 2022	Updates to all sections.
Version 2.1	20 May 2021	Clarified operational responsibilities for Incident Response.
Version 2.2	10 Sep 2021	Added wireless network management practices. Updated Operations Management, Incident Response, Technical Vulnerability Management and Access Control sections.
Version 2.3	22 Apr 2022	Clarified Global Information Security and Incident Response sections



## CONNECT WITH US

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com).

Outside North America, find your local office at [oracle.com/contact](https://www.oracle.com/contact).

 [blogs.oracle.com](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://twitter.com/oracle)

Copyright © 2024, Oracle and/or its affiliates. Unless this document is affirmatively incorporated into Your order for Cloud Services as part of its Service Specifications, the following terms apply:

- This document is provided *for* information purposes only, and the contents hereof are subject to change without notice.
- This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document.
- This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle Corporate Security Practices  
April, 2024

