

ORDER

1. The County of Santa Barbara is issuing this Order to Mythics for the Oracle HCM cloud services provided in accordance with this Order AND the Oracle Public Sector Cloud Services Agreement Terms (“Agreement”).
2. Mythics shall provide the following Oracle software modules listed in Table 1, which are based on the response to the RFP 17-07 by Mythics.

Table 1 - Mythics/Oracle Software Modules		
Public-Cloud Pricing Elements	Vendor Model Number	Description
Fusion Human Capital Management Base Cloud Service	B85800	Hosted Employee
Fusion Goal Management Cloud Service	B67291	Hosted Named User
Fusion Performance Management Cloud Service	B67293	Hosted Named User
Transparent Data Encryption for Oracle Fusion Security Cloud Service	B84494	Each
Oracle Data Visualization Cloud Service	B84522	Hosted Named User
Additional Test Environment for Oracle Fusion Cloud Service	B84490	Each

3. Tables 2 through 10 identify the Human Resources Management System (“HRMS”) functionality to be provided by the Cloud Services and the Oracle software module that will fulfill the HRMS functionality requirement.

Table 2 – Position Management			
Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Position Definitions, Codes & Functions	B85800	Fusion Human Capital Management Base Cloud Service
2.	Position Classifications		
3.	Budgeted		
4.	Non-Budgeted		
5.	Salary		
6.	Filled		
7.	Vacancies		
8.	FTEs		
9.	Other		
10.	Loaned		
11.	Trainees		

Table 2 – Position Management

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
12.	Department		
13.	Division		
14.	Unit		
15.	Location		
16.	Function		
17.	Change Classifications		
18.	Organizational Charts		
19.	Forms and Documents		
20.	Reports, including real time and historical		

Table 3 - Employee Records & Demographics

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Employee Information	B85800	Fusion Human Capital Management Base Cloud Service
2.	Name		
3.	Home Address		
4.	Work Address		
5.	Multiple Telephone Numbers		
6.	Work		
7.	Cell		
8.	Alternate		
9.	Home		
10.	Email		
11.	Work		
12.	Personal		

Table 3 - Employee Records & Demographics

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description		
13.	Emergency Contact Information				
14.	Work Space #				
15.	Unit				
16.	Supervisor name				
17.	Division				
18.	Branch, e.g. Administration, Adult and Children Service				
19.	Department				
20.	Classification				
21.	FTE, Trainee etc.				
22.	County (SBC) Employee ID				
23.	SBC Position Number				
24.	Worker ID for CalWIN #, etc.				
25.	Program			B85800	Fusion Human Capital Management Base Cloud Service
26.	Work Location and address				
27.	Home Address				
28.	IPad				
29.	Mi-Fi				
30.	Laptop				
31.	Cell Phones				
32.	Employment Lifecycle History				
33.	Nepotisms, Relation to any other employee in the County				
34.	Educational Degrees				
35.	Ethnicity				

Table 3 - Employee Records & Demographics

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
36.	Age/DOB		
37.	Generations		
38.	Gender		
39.	Languages		
40.	Years of Experience in Classification		
41.	Non LMS Training Completed, i.e. Red Cross Training or Other Training		
42.	Employee Self-Service - Fields will be determined during the implementation. Explain if there are any limitations.		
43.	Name Changes with alerts		
44.	Manager/Supervisor Self-Service - Fields will be determined during the implementation. Explain if there are any limitations.		
45.	Ability to run reports on the above including real time and historical		

Table 4 – Track Leave of Absence

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Leave of absence begin	B85800	Fusion Human Capital Management Base Cloud Service
2.	Manager/supervisor notification		
3.	Assignment reorientation/ease in		
4.	Updated training requirements		
5.	Update EPR timeline		
6.	Payroll notification		
7.	TrackIT notification		
8.	Facilities notification		

Table 4 – Track Leave of Absence

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
9.	Fiscal notification		
10.	Leave of absence end		
11.	Manager/supervisor notification		
12.	Assignment reorientation/ease in		
13.	Updated training requirements		
14.	Update EPR timeline		
15.	Payroll notification		
16.	TrackIT notification		
17.	Facilities notification		
18.	Fiscal notification		
19.	Reports		

Table 5 - Track Employee Performance Reviews

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Internal due date reminders by unit, division, branch and department	B67293	Fusion Performance Management Cloud service
2.	Evaluation Type		
3.	3 month		
4.	Mid-term		
5.	Mid-term/Merit		
6.	9 Month		
7.	Final Probation		
8.	Annual		
9.	Annual Merit		

Table 5 - Track Employee Performance Reviews

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
10.	IDP check-in		
11.	Check-in		
12.	Performance Evaluation		
13.	Leadership Evaluation		
14.	Special		
15.	PIP		
16.	County due date reminders by unit, division, branch and department		
17.	List of completed employee reviews		
18.	Track all late EPRs		
19.	Reports, ad-hoc, fixed and automated		

Table 6 – Hiring Process

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Offboarding	B85800	Fusion Human Capital Management Base Cloud Service
2.	Create check list for Offboarding		
3.	Attrition by promotions		
4.	Attrition by laterals		
5.	Attrition by demotions		
6.	Attrition by separations		
7.	Exit interviews	B67293	Fusion Performance Management Cloud service
8.	Reasons	B85800	Fusion Human Capital Management Base Cloud Service
9.	Reports		

Table 7 – Budgeting Forecast

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Ability to query the Auditor Controller's budgeting system and extract budget for each budgeted DSS position.	B84522	Oracle Data Visualization Cloud Service

Table 8 – Cross-Check Timesheet

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Timesheet verification by Fiscal department	B84522	Oracle Data Visualization Cloud Service
2.	Employee enters directly into ESS+, timesheet application		
3.	Before it is finalized, Fiscal downloads the information from ESS+ to Excel		
4.	Verification of proper coding of timesheet		
5.	Every two weeks		

Table 9 - Cross-Check Random Moment Sampling (RMS)

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	RMS verification by Fiscal department	B84522	Oracle Data Visualization Cloud Service
2.	Employee enters directly into ESS+, timesheet application		
3.	Fiscal downloads RMS from RMS application		
4.	Verification of proper RMS coding		
5.	Every month		

Table 10 – Lost Time Report

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
1.	Download employee name, ID, available hours, lost times	B84522	Oracle Data Visualization Cloud Service

Table 10 – Lost Time Report

Item No	HRMS Functionality	Bill of Material (BOM)	Oracle Software Module Description
	category hours from DEN into Excel		
2.	Employee Detail by department		
3.	Lost time above average employee exception		
4.	Download from PERS into Excel		
5.	Report on lost time & overtime tracking		

Table 11 is to provide additional software module for the functionality list below:

Table 11 – Additional Software Modules

Item No.	PERS RFP Requirements	Bill of Material (BOM)	Oracle Software Module Description
1.	Data Security and Encryption	B84494	Transparent Data Encryption protects Fusion Applications data which is at rest on the file system from being read or used.
2.	Testing setup before services go online	B84490	This service provides for the hosting and maintenance of an additional Test Environment for non-production use such as development, training and testing activities.
3.	Fusion Goal Management Cloud Service	B67291	To be used in conjunction with B85800.

4. Any notice or consent required or permitted to be given under this Order shall be given to the respective parties in writing, by personal delivery, or with postage prepaid by first class mail, registered or certified mail, or express courier service, as follows:

To COUNTY: Laura Mejia, Department of Social Services,
 304 W. Carmen Lane, Santa Maria, Ca 93455
 (805)614-1252
l.mejia@sbcsocialserv.org

To CONTRACTOR: Ryan Williams, Account Manager, State and Local West, Mythics Inc.
 1439 N. Great Neck Rd. | Virginia Beach, VA 23454
 (757)963-6195
Rwilliams@mythics.com

or at such other address or to such other person that the parties may from time to time designate.

5. The Data Center Region in which Your Services will reside will be in the United States, unless otherwise noted in the Order or, if permissible, as specified by You during provisioning.
6. Oracle HCM Cloud includes Oracle Transactional Business Intelligence (OTBI) which is the tool that allows the County to extract the data from Oracle HCM Cloud and transform it into their required format.
7. Audit performed by Oracle under Section 14.1 of the Agreement shall be at the sole cost and expense of Oracle or Mythics.
 County of Santa Barbara- Order with Mythics, Inc.

8. Notwithstanding anything to the contrary in this Agreement, any modification to the Service Specifications or Program Documentation shall not affect Mythics' or Oracle's obligation to maintain the confidentiality of Your Content, Your Application, or Personal Data to the standard described in Sections 9 and 10 of the Agreement.
9. Additional Terms (attached hereto as Exhibit A), Payment Arrangements (attached hereto as Exhibit B), and Indemnification and Insurance Requirements (attached hereto as Exhibit I) are incorporated herein by reference.
10. Oracle Data Processing Agreement for Oracle Cloud Services (attached hereto as Exhibit "C"), Oracle SaaS Public Cloud Services (attached hereto as Exhibit "D"), Oracle PaaS and IaaS Public Cloud Services (attached hereto as Exhibit "E"), Oracle Cloud Hosting and Delivery Policies (attached hereto as Exhibit "F"), relevant portions of the Oracle Fusion Service Descriptions (attached hereto as Exhibit "G"), and relevant portions of the Oracle PaaS and IaaS Public Cloud Descriptions-Metered & Non-Metered (attached hereto as Exhibit "H") are provided herein for reference only, subject to changes at Oracle discretion. Oracle changes to the aforementioned documents shall not result in a material reduction in the level of performance, security or availability of the applicable Services provided to You.
11. The term of the Order for the Cloud Services is for an initial period of one year to commence upon the installation and provisioning of the Oracle HCM cloud services... County shall have six options to extend the term of the Order for one additional year for each option period. The Agreement terms and conditions shall govern the option periods.
12. Notwithstanding anything to the contrary in this Agreement, in the event that no funds or insufficient funds are appropriated or budgeted by federal, state or county governments, or funds are not otherwise available for payments in the fiscal year(s) covered by the term of this Agreement, then You will notify Mythics of such occurrence and You may terminate or suspend this Agreement in whole or in part, with 30 days notice. Subsequent to termination of this Agreement under this provision, You shall have no obligation to make payments with regard to the remainder of the term.
13. Mythics further understands and acknowledges that it shall not be entitled to any of the benefits of Your employees, including but not limited to vacation, sick leave, administrative leave, health insurance, disability insurance, retirement, unemployment insurance, workers' compensation and protection of tenure. Notwithstanding anything to the contrary in this Agreement, Mythics shall ensure that Oracle will fulfill its obligations under this Agreement, Your Order, Service Specifications, and Program Documentation, and to the extent Oracle does not fulfill its obligations, Mythics shall be held responsible and liable for the obligations of Oracle.

//
Order for Oracle HCM cloud services between the **County of Santa Barbara** and **Mythics, Inc.**

IN WITNESS WHEREOF, the parties have executed this Order to be effective on the date executed by COUNTY.

ATTEST:
Mona Miyasato
County Executive Officer
Clerk of the Board

COUNTY OF SANTA BARBARA:

By: _____
Deputy Clerk

By: _____
Chair, Board of Supervisors

Date: _____

RECOMMENDED FOR APPROVAL:
Department of Social Services

CONTRACTOR:
Mythics, Inc.

By: _____
Department Head

By: _____
Authorized Representative

Name: Dale Darr

Title: VP of Contracts

APPROVED AS TO FORM:
Michael C. Ghizzoni
County Counsel

**APPROVED AS TO ACCOUNTING
FORM:**
Theodore A. Fallati, CPA
Auditor-Controller

By: _____
Deputy County Counsel

By: _____
Deputy

APPROVED AS TO FORM:
Risk Management

By: _____
Risk Management

EXHIBIT A
ADDITIONAL TERMS

1. SCOPE

Mythics agrees to provide the Services to You in accordance with the order AND the Agreement.

2. COMPENSATION

In full consideration for the Services, Mythics shall be paid for performance under this Agreement in accordance with the terms of Exhibit C. Billing shall be made by invoice, which shall include the contract number assigned by You and which is delivered to the address given in Section 19.3 of this Agreement.

3. DEBARMENT AND SUSPENSION

Mythics certifies to You that it and its employees and principals are not debarred, suspended, or otherwise excluded from or ineligible for, participation in federal, state, or county government contracts. Mythics certifies that it shall not contract with a subcontractor that is so debarred or suspended.

4. TAXES

Mythics shall pay all taxes, levies, duties, and assessments of every nature due in connection with any work under this Agreement and shall make any and all payroll deductions required by law. You shall not be responsible for paying any taxes on Mythics' behalf, and should You be required to do so by state, federal, or local taxing agencies, Mythics agree to promptly reimburse You for the full value of such paid taxes plus interest and penalty, if any. These taxes shall include, but not be limited to, the following: FICA (Social Security), unemployment insurance contributions, income tax, disability insurance, and workers' compensation insurance.

5. CONFLICT OF INTEREST

Mythics covenants that it presently has no employment or interest and shall not acquire any employment or interest, direct or indirect, including any interest in any business, property, or source of income, which would conflict in any manner or degree with the Services required to be performed under this Agreement. Mythics further covenants that in the performance of this Agreement, no person having any such interest shall be employed by Mythics. The affected parties must promptly disclose to You, in writing, any potential conflict of interest. You retain the right to waive a conflict of interest disclosed by Mythics if You determine it to be immaterial, and such waiver is only effective if provided by You to Mythics in writing.

6. NO PUBLICITY OR ENDORSEMENT

Mythics shall not use Your name or logo or any variation of such name or logo in any publicity, advertising or promotional materials. Mythics shall not use Your name or logo in any manner that would give the appearance that You are endorsing Mythics. Mythics shall not in any way contract on behalf of or in Your name. Mythics shall not release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning You or Your projects, without obtaining Your prior written approval.

7. RECORDS, AUDIT, AND REVIEW

Mythics shall keep such business records pursuant to this Agreement as would be kept by a reasonably prudent practitioner of Mythics' profession and shall maintain such records for at least four (4) years following the termination of this Agreement. All accounting records shall be kept in accordance with generally accepted accounting principles. You shall have the right to audit and review all such documents and records at any time during Mythics' regular business hours or upon reasonable notice. In addition, if this Agreement exceeds ten thousand dollars (\$10,000.00), Mythics shall be subject to the examination and audit of the California State Auditor, at Your request or as part of any of Your audit, for a period of three (3) years after final payment under the Agreement (Cal. Govt. Code Section 8546.7). Mythics shall participate in any audits and reviews, whether by You or the State, at no charge to You.

If federal, state or county audit exceptions are made relating to this Agreement, Mythics shall reimburse You all costs incurred by federal, state, and/or county governments associated with defending against the audit exceptions or performing any audits or follow-up audits, including but not limited to: audit fees, court costs, attorneys' fees based upon a reasonable hourly amount for attorneys in the community, travel costs, penalty assessments and all other costs of whatever nature. Immediately upon notification from You, Mythics shall reimburse the amount of the audit exceptions and any other related costs directly to You as specified by You in the notification.

8. NONDISCRIMINATION

You hereby notify Mythics that Your Unlawful Discrimination Ordinance (Article XIII of Chapter 2 of the Santa Barbara County Code) applies to this Agreement and is incorporated herein by this reference with the same force and effect as if the ordinance were specifically set out herein and Mythics agrees to comply with said ordinance.

9. NONEXCLUSIVE AGREEMENT

Mythics understands that this is not an exclusive Agreement and that You shall have the right to negotiate with and enter into contracts with others providing the same or similar services as those provided by Mythics as You desire.

10. NO WAIVER OF DEFAULT

No delay or omission by You to exercise any right or power arising upon the occurrence of any event of default shall impair any such right or power or shall be construed to be a waiver of any such default or an acquiescence therein; and every power and remedy given by this Agreement to You shall be exercised from time to time and as often as may be deemed expedient in Your sole discretion.

11. COMPLIANCE WITH LAW

Mythics shall, at its sole cost and expense, comply with all county, state and federal ordinances and statutes now in force or which may hereafter be in force with regard to this Agreement. The judgment of any court of competent jurisdiction, or the admission of Mythics in any action or proceeding against Mythics, whether You are a party thereto or not, that Mythics has violated any such ordinance or statute, shall be conclusive of that fact as between Mythics and You.

12. CALIFORNIA LAW AND JURISDICTION

Notwithstanding anything contrary in this Agreement, this Agreement shall be governed by the laws of the State of California. and any litigation regarding this Agreement or its contents shall be filed in the County of Santa Barbara, if in state court, or in the federal district court nearest to Santa Barbara County, if in federal court, in the event the action is filed by Mythics or County.

13. EXECUTION OF COUNTERPARTS

This Agreement may be executed in any number of counterparts and each of such counterparts shall for all purposes be deemed to be an original; and all such counterparts, or as many of them as the parties shall preserve undestroyed, shall together constitute one and the same instrument.

14. AUTHORITY

All signatories and parties to this Agreement warrant and represent that they have the power and authority to enter into this Agreement in the names, titles and capacities herein stated and on behalf of any entities, persons, or firms represented or purported to be represented by such entity(ies), person(s), or firm(s) and that all formal requirements necessary or required by any state and/or federal law in order to enter into this Agreement have been fully complied with. Furthermore, by entering into this Agreement, Mythics hereby warrants that it shall not have breached the terms or conditions of any other contract or agreement to which Mythics is obligated, which breach would have a material effect hereon.

15. SURVIVAL

All provisions of this Agreement which by their nature are intended to survive the termination or expiration of this Agreement shall survive such termination or expiration.

16. STATE ENERGY CONSERVATION PLAN

Mythics agrees to comply with mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6201).

17. PROHIBITION OF EXPENDING LOCAL AGENCY STATE OR FEDERAL FUNDS FOR LOBBYING

A. Mythics, by signing this Agreement, hereby certifies to the best of his, her or its knowledge and belief that:

1. No state, federal or local agency appropriated funds have been paid, or will be paid by-or-on behalf of Mythics to any person for influencing or attempting to influence an officer or employee of any state or federal agency; a Member of the State Legislature or United States Congress; an officer or employee of the Legislature or Congress; or any employee of a Member of the Legislature or Congress, in connection with the awarding of any state or federal contract; the making of any state or federal grant; the making of any state or federal loan; the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any state or federal contract, grant, loan, or cooperative agreement.

2. If any funds other than federal appropriated funds have been paid, or will be paid to any person for influencing or attempting to influence an officer or employee of any federal agency; a Member of Congress; an officer or employee of Congress, or an employee of a Member of Congress; in connection with this federal contract, grant, loan, or cooperative agreement; Mythics shall complete and submit California State Standard Form-LLL, "Disclosure Form to Report Lobbying," to You and in accordance with the instructions found therein.

B. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

C. Mythics also agrees by signing this document that it shall require that the language of this certification be included in all lower-tier subcontracts, which exceed \$100,000 and that all such sub recipients shall certify and disclose accordingly.

18. CLEAN AIR ACT AND FEDERAL WATER POLLUTION CONTROL ACT

Mythics shall comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and pursuant to the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Mythics shall promptly disclose, in writing, to You office, to the Federal Awarding Agency, and to the Regional Office of the Environmental Protection Agency (EPA), whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, Mythics has credible evidence that a principal, employee, agent, or subcontractor of Mythics has committed a violation of the Clean Air Act (42 U.S.C. 7401-7671q.) or the Federal Water Pollution Control Act (33 U.S.C. 1251-1387).

19. MANDATORY DISCLOSURE

Mythics must disclose, in a timely manner, in writing to You all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the award. Mythics is required to report certain civil, criminal, or administrative proceedings to the System for Award Management (SAM) located at www.sam.gov. Failure to make required disclosures can result in any of the remedies described in 2 CFR §200.338 Remedies for noncompliance, including suspension or debarment. (See also 2 CFR part 180 and 31 U.S.C. 3321.)

EXHIBIT B

PAYMENT ARRANGEMENTS

1. For Services to be rendered under this Agreement, Mythics shall be paid a total contract amount, including cost reimbursements, not to exceed \$131,051.64 for the initial one-year period. If all option years are exercised per Section 11 of the Order, the total contract amount, including cost reimbursements, of the 6 option years, shall not exceed \$831,090.89, which is based on the yearly and monthly not to exceed totals listed below. The total amount including option years is \$962,142.53.

The yearly and monthly not to exceed totals of the software modules for Year 1 shall be:

Total Year 1: \$131,051.64 (monthly \$10,920.97)

The yearly and monthly not to exceed totals of the software modules for the option Years 2 to 7 (if options are exercised) shall be:

Total Year 2: \$131,051.64 (monthly \$10,920.97)

Total Year 3: \$131,051.64 (monthly \$10,920.97)

Total Year 4: \$134,983.19 (monthly \$11,248.60)

Total Year 5: \$139,032.68 (monthly \$11,586.06)

Total Year 6: \$144,593.99 (monthly \$12,049.50)

Total Year 7: \$150,377.75 (monthly \$12,531.48)

The yearly price is based on 1019 Users, as applicable.

The total contract amount is based on the software module pricing in Table 1.

Table I - Mythics/Oracle Contract Pricing								
Public-Cloud Pricing Elements	Vendor Model Number		Unit Price	% Discount	Unit Price After Discount	Total No. of Units	Total Price/Year	Monthly Recurring Price
Fusion Human Capital Management Base Cloud Service	B85800	Hosted Employee	\$156.00	61.00%	\$60.84	1019	\$61,995.96	\$5,166.33
Fusion Goal Management Cloud Service	B67291	Hosted Named User	\$24.00	61.00%	\$9.36	1019	\$9,537.84	\$794.82
Fusion Performance Management Cloud Service	B67293	Hosted Named User	\$24.00	61.00%	\$9.36	1019	\$9,537.84	\$794.82
Transparent Data Encryption for Oracle Fusion Security Cloud Service	B84494	Each	\$25,000.00	61.00%	\$9,750.00	1	\$9,750.00	\$812.50
Oracle Data Visualization Cloud Service	B84522	Hosted Named User	\$900.00	39.00%	\$549.00	20	\$10,980.00	\$915.00
Additional Test Environment for Oracle Fusion Cloud Service	B84490	Each	\$75,000.00	61.00%	\$29,250.00	1	\$29,250.00	\$2,437.50

In no event shall the overall budget amount be exceeded without a formal amendment to this Agreement.

2. Quarterly, Mythics shall submit to the COUNTY an invoice or certified claim on the County Treasury for the service performed over the period specified. These invoices or certified claims must cite the assigned Board Contract Number. COUNTY shall pay invoices or claims within 30 days of receipt of correct and complete invoices or claims from Mythics.

EXHIBIT C

DATA PROCESSING AGREEMENT FOR ORACLE CLOUD SERVICES

Data Processing Agreement for Oracle Cloud Services

Version March 1, 2017

1. Scope and order of precedence

This data processing agreement (the "Data Processing Agreement") applies to Oracle's Processing of Personal Data provided to Oracle by Customer as part of Oracle's provision of Cloud Services ("Cloud Services"). The Cloud Services are specified in (i) the applicable Oracle Cloud Services Agreement or other applicable master agreement and (ii) the Oracle Cloud Order and all documents, addenda, schedules and exhibits incorporated therein (collectively the "Agreement") by and between Customer and the Oracle subsidiary listed in the Oracle Cloud Order.

This Data Processing Agreement is incorporated into and subject to the terms of the Agreement. Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement, including any policies or schedules referenced therein, and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall take precedence.

This Data Processing Agreement shall be effective for the Service Period of any Oracle Cloud order placed under the Agreement.

2. Definitions

"Controller" and "Processor" have the meaning set forth in the Directive.

"Customer" means the Customer that has executed the Oracle Cloud Order.

"Data Subject" means an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

"Directive" means Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.

"Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive.

"Oracle" or "Processor" means the Oracle subsidiary listed in the Oracle Cloud Order.

"Oracle Affiliates" mean the subsidiaries of Oracle Corporation that may assist in the performance of the Cloud Services.

"Personal Data" means any information relating to a Data Subject that Customer or its end users provide to Oracle as part of the Cloud Services.

"Process" or "Processing" means any operation or set of operations which is performed by Oracle as part of the Cloud Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Third Party Subprocessor" means a third party subcontractor, other than an Oracle Affiliate,

engaged by Oracle which, as part of the subcontractor's role of delivering the Cloud Services, will Process Personal Data of the Customer.

Other terms have the definitions provided for them in the Agreement or as otherwise specified below.

3. Categories of Personal Data

In order to execute the Agreement, and in particular to perform the Cloud Services, Customer authorizes and requests that Oracle Process the following Personal Data:

Categories of Personal Data: Personal Data may include, among other information, 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, social security details and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

Categories of Data Subjects: Data subjects may include Customer's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, customers and users of the Customer. Data subjects also may include individuals attempting to communicate or transfer Personal Data to users of the Cloud Services.

4. Customer's Instructions

Customer may provide instructions in writing to Oracle in addition to those specified in the Agreement with regard to Processing of Personal Data. Oracle will comply with all such instructions without additional charge to the extent necessary for Oracle to comply with its obligations as a Processor in the performance of the Cloud Services. The parties will negotiate in good faith with respect to any other change in the Cloud Services and/or fees resulting from any additional instructions.

5. Controller and Processor of Personal Data and purpose of the Personal Data Processing

Customer will at all times remain the Controller for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Customer is responsible for compliance with its obligations as a Controller under data protection laws, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents and authorizations), and for its decisions and actions concerning the Processing and use of the Personal Data.

Oracle is a Processor for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Oracle will Process Personal Data solely for the provision of the Cloud Services, and will not otherwise (i) Process or use Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in accordance with Section 4, or (ii) disclose such Personal Data to third parties other than Oracle Affiliates or Third Party Subprocessors for the aforementioned purposes or as required by law.

Oracle will comply with all applicable data protections laws to the extent that such laws by their terms impose obligations directly upon Oracle as a Processor in connection with the services specified in the applicable Cloud Order.

6. Rights of Data Subjects

Oracle will grant Customer electronic access to Customer's Cloud Services environment that holds Personal Data to permit Customer to respond to Data Subject requests to access, delete, release,



correct or block access to specific Personal Data.

To the extent such electronic access is not available to Customer, Oracle will follow Customer's detailed written instructions to access, delete, release, correct or block access to Personal Data held in Customer's Cloud Services environment. Customer agrees to pay Oracle's reasonable fees that may be associated with Oracle's performance of any such access, deletion, release, correction or blocking of access to Personal Data on behalf of Customer.

Oracle will pass on to the Customer any requests of an individual Data Subject to access, delete, release, correct or block Personal Data Processed under the Agreement. Oracle will not be responsible for responding directly to the request, unless otherwise required by law.

7. Cross Border and Onward Data Transfers

Oracle treats all Personal Data in a manner consistent with the requirements of the Agreement and this Data Processing Agreement in all locations globally. Oracle's information, privacy and security policies, standards and governance practices are managed on a global basis.

Transfers of Personal Data originating from the EEA or Switzerland to Oracle Affiliates or Third Party Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national data protection authority, are subject to (i) the terms of the Model Clauses; or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the Directive. The terms of this Data Processing Agreement shall be read in conjunction with the Model Clauses or other appropriate transfer mechanisms.

Transfers of Personal Data originating from other locations globally to Oracle Affiliates or Third Party Subprocessors are subject to (i) for Oracle Affiliates, the terms of the Oracle Intra-Company Data Processing and Transfer Agreement entered into between Oracle Corporation and the Oracle Affiliates, which requires all transfers of Personal Data to be made in compliance with all applicable Oracle security and data privacy policies and standards; and (ii) for Third Party Subprocessors, the terms of the relevant Oracle Third Party Subprocessor agreement incorporating security and other data privacy requirements consistent with those of this Data Processing Agreement.

8. Affiliates and Third Party Subprocessors

Some or all of Oracle's obligations under the Agreement may be performed by Oracle Affiliates and Third Party Subprocessors. Oracle maintains a list of Oracle Affiliates and Third Party Subprocessors that may Process Personal Data. That list will be available to Customer via the Cloud portal or, to the extent Customer has no access to the Cloud portal, Oracle will provide a copy of that list to Customer upon request.

The Oracle Affiliates and Third Party Subprocessors are required to abide by substantially the same obligations as Oracle under this Data Processing Agreement as applicable to their Processing of Personal Data. Customer may request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to ensure compliance with such obligations. Customer will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with Third Party Subprocessors that may Process Personal Data.

Oracle remains responsible at all times for compliance with the terms of this Data Processing Agreement by Oracle Affiliates and Third Party Subprocessors.

Customer consents to Oracle's use of Oracle Affiliates and Third Party Subprocessors in the

performance of the Cloud Services in accordance with the terms of Sections 7 and 8 above.

9. Technical and Organizational Measures

Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data, including the measures specified in this Section to the extent applicable to Oracle's Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Cloud Services ordered by Customer, may be specified in the Agreement.

9.1 Physical Access Control. Oracle employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is Processed, such as the use of security personnel, secured buildings and data center premises.

9.2 System Access Control. The following may, among other controls, be applied depending upon the particular Cloud Services ordered: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Services hosted at Oracle: (i) log-ins to Cloud Services Environments by Oracle employees and Third Party Subprocessors are logged; (ii) logical access to the data centers is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.

9.3 Data Access Control. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. In addition to the access control rules set forth in Sections 9.1 – 9.3, Oracle implements an access policy under which Customer controls access to its Cloud Services environment and to Personal Data and other data by its authorized personnel.

9.4 Transmission Control. Except as otherwise specified for the Cloud Services (including within the Oracle Cloud Order or the applicable service specifications referenced in the Agreement), transmissions of data outside the Cloud Service environment are encrypted. Some Cloud Services, such as social media services, may be configurable by Customer to permit access to third party sites that require unencrypted communications. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. Customer is solely responsible for the results of its decision to use such unencrypted communications or transmissions.

9.5 Input Control. The Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer. As set forth in Section 9.4 above, note that some Cloud Services permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

9.6 Data Backup. For Cloud Services hosted at Oracle: back-ups are taken on a regular basis; back-ups are secured using a combination of technical and physical controls, depending on the particular Cloud Service.

9.7 Data Segregation. Personal Data from different Oracle customers' environments is logically segregated on Oracle's systems.

9.8 Confidentiality. All Oracle employees and Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements.

10. Audit Rights

Customer may audit Oracle's compliance with the terms of this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Cloud Service data center facility that Processes Personal Data to the extent required by laws applicable to Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and Oracle and must execute a written confidentiality agreement acceptable to Oracle before conducting the audit.

To request an audit, Customer must submit a detailed audit plan to Oracle at least two weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Oracle security, privacy, employment or other relevant policies). Oracle will work cooperatively with Customer to agree on a final audit plan. If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve months and Oracle confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

The audit must be conducted during regular business hours at the applicable facility, subject to Oracle policies, and may not unreasonably interfere with Oracle business activities.

Customer will provide Oracle any audit reports generated in connection with any audit under this Section 10, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits are at the Customer's expense. Any request for Oracle to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Cloud Services. Oracle will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

11. Incident Management and Breach Notification

Oracle evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or handling of Personal Data ("Incident"). Oracle operations staff is instructed on responding to Incidents where processing of Personal Data may have been unauthorized, including prompt and reasonable internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence.

Depending on the nature of the Incident, Oracle defines escalation paths and response teams to address the Incident. Oracle will work with Customer, with internal Oracle lines of business, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the Incident. The goal of Oracle's Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment, and to establish root causes and remediation steps.

For purposes of this section, "Security Breach" means the misappropriation or unauthorized Processing of Personal Data located on Oracle systems or the Cloud Services environment, including by an Oracle employee, that compromises the security, confidentiality or integrity of such Personal Data. Oracle will inform Customer within 24 hours or sooner as required by applicable law if Oracle determines that Personal Data has been subject to a Security Breach or any other circumstance in which Customer is required to provide a notification under applicable law.

Oracle will promptly investigate the Security Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by law, Oracle will provide Customer with a description of the Security Breach, the type of



Personal Data that was the subject of the Security Breach, and other information Customer may reasonably request concerning the affected Data Subjects. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant data protection authorities.

12. Return and Deletion of Personal Data upon End of Cloud Services

Following termination of the Cloud Services, Oracle will return or otherwise make available for retrieval Customer's Personal Data then available in the Customer's Cloud Services environment. Following return of such Personal Data, or as otherwise specified in the Agreement, Oracle will promptly delete or otherwise render inaccessible all copies of Personal Data from the production Cloud Services environment, except as may be required by law. Oracle's data return and deletion practices are described in more detail in the Agreement.

13. Legally Required Disclosures

Except as otherwise required by law, Oracle will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority ("Demand") that it receives and which relates to the Processing of Personal Data. At Customer's request, Oracle will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Oracle has no responsibility to interact directly with the entity making the Demand.

14. Service Analyses

Oracle may (i) compile statistical and other information related to the performance, operation and use of the Cloud Services, and (ii) use data from the Cloud Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (collectively "Service Analyses"). Oracle may make Service Analyses publicly available. However, Service Analyses will not incorporate Customer's Content, Personal Data or Confidential Information in a form that could identify or serve to identify Customer or any Data Subject. Oracle retains all intellectual property rights in Service Analyses.

EXHIBIT D

ORACLE SAAS PUBLIC CLOUD SERVICES

ORACLE CLOUD

Oracle SaaS Public Cloud Services

PILLAR DOCUMENTATION | APRIL 2017



Table of Contents

Scope	1
Oracle Cloud Security Policy	1
Physical Security Safeguards	1
Oracle Cloud Service Level Objective Policy	1
Target Service Availability Level	1
Oracle Cloud Services Continuity Policy	1
Oracle Cloud Services Backup Strategy	1
Disaster Recovery for Oracle SaaS Public Cloud Services	1
Oracle Cloud Service Level Objective Policy	3
Customer Monitoring & Testing Tools	3
Oracle Cloud Change Management Policy	3
Oracle Cloud Support Policy	4
Cloud Customer Support Portal	4
Oracle Cloud Suspension and Termination Policy	4



Scope

This document applies to Oracle SaaS Public Cloud Services purchased by You, and supplements the *Oracle Cloud Hosting and Delivery Policies* incorporated into Your order.

Oracle Cloud Security Policy

Physical Security Safeguards

For LogFire Warehouse Management Cloud Products, the following applies in lieu of the text in section 1.3 of the Oracle Cloud Hosting and Delivery Policies:

In accordance with reasonable practices, Oracle provides secured computing facilities for both office locations and production cloud infrastructure.

Oracle Cloud Service Level Objective Policy

Target Service Availability Level

For purposes of calculating the Service Availability Level of the Oracle SaaS Public Cloud Services, "Available" or "Availability" means that You and Your Users are able to log in and access the OLTP or transactional portion of Cloud Services.

The Target Service Availability Levels (or Target Uptimes) for Oracle SaaS Public Cloud Services are set forth in, and subject to, the Oracle Cloud Service Level Objective Policy of the *Oracle Cloud Hosting and Delivery Policies* document, except as follows Oracle works to meet a Target Service Availability Level of 99.9% for the production Oracle Responsys Automatic Failover for Transactional Messages Cloud Service, over the measurement period of one calendar month, commencing at Oracle's activation of the production environment.

Oracle works to meet a Target Service Availability Level of 99.9% for the production Oracle Commerce Cloud Service, over the measurement period of one calendar month, commencing at Oracle's activation of the production environment.

Oracle Cloud Services Continuity Policy

Oracle Cloud Services Backup Strategy


For the Oracle Responsys Cloud Service, a backup is retained for a period of at least 21 days after the date that the backup is made.

For the Oracle Content Marketing Cloud Service, a backup is retained for a period of at least 30 days after the date that the backup is made.

For the Push Cloud Service, a backup is retained for a period of at least 7 days after the date that the backup is made.

For the Oracle Maxymiser Cloud Service, a backup is retained for a period of at least 30 days after the date that the backup is made.

Disaster Recovery for Oracle SaaS Public Cloud Services



Disaster Recovery (DR) services for Oracle SaaS Public Cloud Services are intended to provide service restoration capability in the event of a major disaster, as declared by Oracle. Oracle will determine whether an event constitutes a disaster requiring the execution of the DR plan for the affected service.

Oracle will work to perform DR services for Oracle SaaS Public Cloud Services as described below.

For Remote Cloud Services, Oracle will work to provide DR services for the SaaS Public Cloud Service on the underlying platform, contingent on You first: 1) performing the following to support disaster recovery in accordance with the DR plan: 2) providing a secondary data center site with network connectivity of sufficient bandwidth as determined by Oracle, between Your primary and disaster recovery sites; and 3) purchasing sufficient additional services deployed at Your secondary site for disaster recovery purposes (e.g., an adequate number and type of Oracle Public Cloud Machines and SaaS Public Cloud Service subscriptions on that platform). Oracle Public Cloud Machine and other Oracle Cloud Services that are deployed on Oracle Public Cloud Machine as the underlying platform, are examples of Remote Cloud Services.

Recovery Time Objective: Recovery time objective (RTO) is Oracle's objective for the maximum period of time between Oracle's decision to activate the DR recovery processes described in this document to failover the Oracle SaaS Public Cloud Service to a secondary site due to a declared disaster, and the point at which You can resume production operations in the standby production environment at the secondary site. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO objective for each Oracle SaaS Public Cloud Service is described in this document below or is otherwise stated in the service description of the applicable Cloud Service.

Recovery Point Objective: Recovery point objective (RPO) is Oracle's objective for the maximum period of data loss measured as the time from which the first transaction is lost until Oracle's declaration of the disaster. The RPO does not apply to any data loads that are underway when the disaster occurs. The RPO objective for each Oracle SaaS Public Cloud Service is described in this document below or is otherwise stated in the service description of the applicable Cloud Service.


The RTO and RPO objectives do not apply to customizations that depend on external components or third-party software. During an active failover event or recovery operations, non-critical fixes and enhancement requests are not supported. Oracle is not responsible for issues arising from third party software and customizations to Oracle programs and services.

Upon Oracle's declaration of a disaster for the following services Oracle will commence its Disaster Recovery plan to recover the production environments of the affected Cloud Services in accordance with the RTO and RPO Objectives specified for each service listed below. Production services may operate in a degraded state of performance for the duration of the disaster event.

The RTO is **12 hours** and the RPO is **1 hour** for the following services:

1. Oracle Fusion Customer Relationship Management Cloud Service
2. Oracle Fusion Human Capital Management Cloud Service
3. Oracle Fusion Enterprise Resource Planning Cloud Service
4. Oracle Taleo Enterprise Cloud Service
5. Oracle RightNow Cloud Service
6. Oracle Big Machines CPQ Cloud Service
7. LogFire Warehouse Management Cloud Products*

*For LogFire Warehouse Management Cloud Products, in the **UK Data Center Region**, in the event of a declared disaster, Oracle will commence its Disaster Recovery plan to recover the production environments of the affected Oracle Cloud Service in an alternative Data Center Region (Dallas, USA).



The RTO is 5 hours and the RPO is **1 hour** for the following service:

8. Oracle Field Service Cloud Service

The RTO is **30 minutes** and the RPO is **15 minutes** for the following service:

9. Oracle Responsys Automatic Failover for Transactional Messages Cloud Service

Upon Oracle's declaration of a disaster for the following services, Oracle will deploy commercially reasonable efforts to recover the production environments of the affected Cloud Services. Production services may operate in a degraded state of performance for the duration of the disaster event. The Recovery Time Objectives and Recovery Point Objectives do not apply to the following Oracle Cloud Services.

10. Oracle Marketing Cloud Service
11. Oracle Commerce Cloud Service
12. Oracle Eloqua & Content Marketing Cloud Service
13. Maxymiser Cloud Service
14. Enterprise Performance Management Cloud Service
15. Oracle Transactional Business Intelligent Enterprise Cloud Service
16. Oracle Transportation Management Cloud Service
17. Oracle Global Trade Management Cloud Service
18. Oracle Responsys Cloud Service
19. Oracle Social Relationship Management Cloud Service
20. Oracle Social Data & Insight Cloud Service
21. Oracle Taleo Business Edition Cloud Service
22. Oracle Taleo Learn Cloud Service
23. Oracle Customer Experience for Midsize Cloud Service
24. Oracle Human Capital Management for Midsize Cloud Service
25. Oracle Enterprise Resource Planning for Midsize Cloud Service


For all Cloud Services in the **South America Data Center Region**, in the event of a declared disaster, Oracle will activate processes to recover the production environment of the affected Oracle Cloud Service in an alternative Data Center Region and will work to restore production data from the most recent available backup made prior to the onset of the disaster. Although Oracle will work to recover the service promptly, the nature of the disaster may affect the time period within which the service can be recovered. The Recovery Time and Recovery Point Objectives do not apply to Oracle Cloud Services in the South America Data Center Region.

Oracle Cloud Service Level Objective Policy

Customer Monitoring & Testing Tools

This section does not apply to the Oracle RightNow CoBrowse Service.

Oracle Cloud Change Management Policy



The scheduled maintenance periods for the Oracle SaaS Public Cloud Services are documented on My Oracle Support in Knowledge Article 1681146.1: <https://support.oracle.com/epmos/faces/DocumentDisplay?id=1681146.1>.

This policy does not apply to the Oracle RightNow CoBrowse Service.

Oracle Cloud Support Policy

For LogFire Warehouse Management Cloud Products, the following applies in lieu of the text in section 5.1.4 of the Oracle Hosting and Delivery policy:

Support for LogFire Warehouse Management Cloud Products is provided through the designated [Cloud Customer Support Portal](#), and consists of:

- Diagnosis of problems or issues with the Oracle Cloud Services.
- Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that they perform in all material respects as described in the associated Program Documentation.
- Support during Change Management activities described in the Oracle Cloud Change Management Policy.
- Assistance with technical service requests 10 hours per day, 5 business days per week, excluding holidays. For Advanced and Premium Support offerings, assistance with service requests is available 24 hours per day, 7 days a week, for an additional fee. Premium Support includes an assigned Support Engineer and onsite support. Please speak to your Oracle Sales Representative for more information.
- Oracle will use reasonable efforts to respond to Severity 1 service requests within sixty (60) minutes of an issue being logged with LogFire during local business hours.
- 24 x 7 access to a Cloud Customer Support Portal designated by Oracle.
- Online Support Coverage, Support Telephone numbers and the Support email address are available via <https://www.oracle.com/corporate/acquisitions/logfire/support.html>

The following sections of the Oracle Cloud Support Policy do not apply to LogFire Warehouse Management Cloud Products: sections 5.2.2 and 5.3 of the Oracle Cloud Hosting and Delivery Policies.

Cloud Customer Support Portal

The Oracle Maxymiser Cloud Service does not use the service notification or alert feature of the Cloud Customer Support Portal.

Oracle Cloud Suspension and Termination Policy

This policy does not apply to the Oracle RightNow CoBrowse Service.



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.


 | Oracle is committed to developing practices and products that help protect the environment

EXHIBIT E

ORACLE PAAS AND IAAS PUBLIC CLOUD SERVICES

Oracle PaaS and IaaS Public Cloud Services

PILLAR DOCUMENTATION JUNE 2017



Table of Contents

Table of Contents	1
Scope	1
Oracle Cloud Service Level Objective Policy: Target Service Uptime	1
Category 1	1
Category 2	1
Category 3	2
Category 4	3
Category 5	3
Category 6	4
Oracle Cloud Security Policy	4
Physical Security Safeguards	4
Oracle Cloud Service Continuity Policy	4
Oracle Cloud Services High Availability Strategy	4
Oracle Cloud Change Management Policy	5
Emergency Maintenance	5
Data Center Migrations	5
Oracle Cloud Support Policy	5
Oracle Cloud Suspension and Termination Policy	5



Scope

This document applies to Oracle PaaS and IaaS Public Cloud Services purchased by You, and supplements the *Oracle Cloud Hosting and Delivery Policies* incorporated into Your order.

Oracle Cloud Service Level Objective Policy: Target Service Uptime

Following the end of each calendar month of the applicable Services Period, Oracle measures the Service Availability Level or Service Uptime for Oracle PaaS and IaaS Public Cloud Services over the immediately preceding month. The Target Service Uptime for Oracle PaaS and IaaS Public Cloud Services, as well as the calculation of the measured Service Uptime and definition of Unplanned Downtime, is set forth in and subject to the Oracle Cloud Service Level Objective Policy of the *Oracle Cloud Hosting and Delivery Policies* and as otherwise defined below for specific categories of Oracle PaaS and IaaS Public Cloud Services.

Category 1

Service Commitment

Commencing at Oracle's activation of the applicable Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.95% for the following:

1. Oracle Database Cloud Service
2. Oracle Java Cloud Service
3. Oracle Application Container Cloud Service
4. Oracle SOA Cloud Service
5. Oracle API Manager Cloud Service
6. Oracle Managed File Transfer Cloud Service
7. Oracle Database Exadata Cloud Service
8. Oracle GoldenGate Cloud Service
9. Oracle MySQL Cloud Service
10. Oracle Data Integrator Cloud Service
11. Oracle WebCenter Portal Cloud Service
12. Oracle Event Hub Cloud Service
13. Oracle Big Data Cloud Service – Compute Edition
14. Oracle Bare Metal Cloud Database Service
15. Oracle API Platform Cloud Service

Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 1:

1. "Unavailable" or "Unavailability" means:
 - a. Any time during which a problem with the Oracle PaaS and IaaS Public Cloud Service prevents external connectivity to any of Your instances.

Category 2

Service Commitment

Commencing at Oracle's activation of the Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.9% for the following:

1. Oracle Database Backup Service
2. Oracle Storage Cloud Service
3. Oracle Bare Metal Cloud Object Storage Service



Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 2:

1. "Service Uptime" is measured by Oracle over the immediately preceding month by subtracting from 100 the addition of the Error Rate of each hour of that month, dividing the sum of those Error Rates by the total number of hours in that month, and multiplying the result by 100 to reach a percent figure.
2. "Error Rate" is the total number of Failed Service REST API Calls in a one-hour time interval in the measured month of the Services Period divided by the total number of Service REST API Calls during that one-hour time interval.
3. A "Service REST API Call" is any HTTP Request that fulfills the service's REST API specification.
4. A "Failed Service REST API Call" is any Service REST API Call processed by Your User that results in a 5xx (Server Error) class of status code.

Category 3

Service Commitment

Commencing at Oracle's activation of the Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.95% for the following:

1. Oracle Messaging Cloud Service
2. Oracle Database Cloud Service – Multitenant Edition
3. Oracle Java Cloud Service – SaaS Extension
4. Oracle Application Builder Cloud Service
5. Oracle Business Intelligence Cloud Service
6. Oracle Data Visualization Cloud Service
7. Oracle Documents Cloud Service
8. Oracle Sites Cloud Service
9. Oracle Integration Cloud Service
10. Oracle Internet of Things Cloud Service
11. Oracle Internet of Things Cloud Service – Enterprise
12. Oracle Internet of Things Production Monitoring Cloud Service
13. Oracle Internet of Things Asset Monitoring Cloud Service
14. Oracle Application Performance Monitoring Cloud Service
15. Oracle IT Analytics Cloud Service
16. Oracle Log Analytics Cloud Service
17. Oracle Mobile Cloud Service
18. Oracle Process Cloud Service
19. Oracle Big Data Preparation Cloud Service
20. Oracle Big Data Discovery Cloud Service
21. Oracle Database Exadata Express Cloud Service
22. Oracle Identity Cloud Service
23. Oracle CASB Cloud Service
24. Oracle Analytics Cloud
25. Oracle Bare Metal Cloud Identity and Access Management Service



Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 3:

1. "Unavailable" or "Unavailability" means:
 - a. Any time during which a problem with the Oracle PaaS and IaaS Public Cloud Service prevents external connectivity for all Your instances.

Category 4

Service Commitment

Commencing at Oracle's activation of the Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.95% for the following:

1. Oracle Big Data Cloud Service – Starter Pack – 3 Nodes
2. Oracle Big Data SQL Cloud Service

Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 4:

1. "Unavailable" or "Unavailability" means:
 - a. Any time during which a problem with the Oracle PaaS and IaaS Public Cloud Service prevents external connectivity for all Your nodes.

Category 5

Service Commitment

Commencing at Oracle's activation of the Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.95% for the following:

1. Oracle Compute Cloud Service
2. Oracle Container Cloud Service
3. Oracle Public Cloud Machine
4. Oracle Database Exadata Cloud Machine
5. Oracle ZS5 Storage Public Cloud Machine
6. Oracle Ravello Cloud Service
7. Oracle Compute Cloud Service – Dedicated Compute
8. Oracle Compute Cloud Service – Load Balancer
9. Oracle Bare Metal Cloud Compute Service
10. Oracle Bare Metal Cloud Block Volume Service
11. Oracle Bare Metal Cloud Load Balancing Service

Note: Oracle Public Cloud Machine, Oracle Database Exadata Cloud Machine, Oracle ZS5 Storage Public Cloud Machine and Oracle Big Data Cloud Machine are examples of Oracle Remote Cloud Services.



Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 5:

1. "Unavailable" or "Unavailability" means:
 - a. Any time during which a problem with the Oracle PaaS and IaaS Public Cloud Service prevents:
 - a. external connectivity for all Your instances, and
 - b. access to Your attached block storage volumes.

Category 6

Service Commitment

Commencing at Oracle's activation of the Oracle PaaS and IaaS Public Cloud Service, Oracle works to meet the Target Service Uptime of 99.9% for the following:

1. Oracle Network Cloud Service

Definitions

The following definitions apply for purposes of calculating the Service Uptime of the Oracle PaaS and IaaS Public Cloud Services included within this Category 6:

1. "Unavailable" or "Unavailability" means:
 - a. Any time during which a problem with the Oracle PaaS and IaaS Public Cloud Service prevents external IP level connectivity for all the Oracle PaaS and IaaS Public Cloud Services that are configured for access via FastConnect.

"Unavailable" or "Unavailability" does not include any time during which the Oracle PaaS and IaaS Public Cloud Services or any service component are unavailable as caused by or resulting from Your Network Service Provider or Equinix Cloud Exchange.


Oracle Cloud Security Policy

Physical Security Safeguards

For Oracle Ravello Cloud Services and Oracle CASB Cloud Services, the following applies in lieu of the text in section 1.3 of the *Oracle Cloud Hosting and Delivery Policies*: Oracle provides secured computing facilities for both office locations and production cloud infrastructure.

Oracle Cloud Service Continuity Policy

Oracle Cloud Services High Availability Strategy



For Oracle CASB Cloud Services, the following applies in lieu of the text in section 2.1 of the *Oracle Cloud Hosting and Delivery Policies*: Oracle CASB Cloud Services are designed to maintain service availability in the case of an incident affecting the services.

Oracle Cloud Change Management Policy

The scheduled maintenance periods for the Oracle PaaS and IaaS Public Cloud Services are documented on My Oracle Support in Knowledge Article 1681146.1:
<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1681146.1>.

Emergency Maintenance

For Oracle Ravello Cloud Services, the following applies in lieu of the text in section 4.1.1 of the *Oracle Cloud Hosting and Delivery Policies*: Oracle will work to provide prior notice for any emergency maintenance requiring a service interruption.

Data Center Migrations

For Oracle Ravello Cloud Services, the following applies in lieu of the text in section 4.1.3 of the *Oracle Cloud Hosting and Delivery Policies*: For data center migrations for purposes other than disaster recovery, Oracle will provide prior notice to You.

Oracle Cloud Support Policy

For FUJITSU Cloud Service K5 DB powered by Oracle® Cloud service, Fujitsu provides first level support to customers by responding to technical inquiries and incidents reported by customers via email and telephone. Oracle provides second line support in case the technical inquires and incidents cannot be solved by Fujitsu.

Oracle Cloud Suspension and Termination Policy

The second paragraph of section 6.1 of the *Oracle Cloud Hosting and Delivery Policies* does not apply to Oracle Ravello Cloud Services.







Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

 | Oracle is committed to developing practices and products that help protect the environment

EXHIBIT F

ORACLE CLOUD HOSTING AND DELIVERY POLICIES

Oracle Cloud Hosting and Delivery Policies

DECEMBER 2016

VERSION 2.2



Table of Contents

1	Oracle Cloud Security Policy	1
1.1	Oracle Information Security Practices - General	1
1.2	User Encryption for External Connections	2
1.3	Physical Security Safeguards	2
1.4	Oracle Software Security Assurance	2
1.5	Customer Security Related Obligations	2
2	Oracle Cloud Service Continuity Policy	3
2.1	Oracle Cloud Services High Availability Strategy	3
2.2	Oracle Cloud Services Backup Strategy	3
3	Oracle Cloud Service Level Objective Policy	3
3.1	Hours of Operation	3
3.2	Service Availability	3
3.2.1	Measurement of Availability	3
3.2.2	Reporting of Availability	4
3.3	Definition of Unplanned Downtime	4
3.4	Monitoring	4
3.4.1	Monitored Components	5
3.4.2	Customer Monitoring & Testing Tools	5
4	Oracle Cloud Change Management Policy	5
4.1	Oracle Cloud Change Management and Maintenance	5
4.1.1	Emergency Maintenance	6
4.1.2	Major Maintenance Changes	6
4.1.3	Data Center Migrations	6
4.2	Software Versioning	6
4.2.1	Software Upgrades and Updates	6
4.2.2	End of Life	6

5	Oracle Cloud Support Policy	7
5.1	Oracle Cloud Support Terms	7
5.1.1	Support fees	7
5.1.2	Support period	7
5.1.3	Technical contacts	7
5.1.4	Oracle Cloud Support	7
5.2	Oracle Cloud Customer Support Systems	7
5.2.1	Cloud Customer Support Portal	7
5.2.2	Live Telephone Support	8
5.3	Severity Definitions	8
5.4	Change to Service Request Severity Level	8
5.4.1	Initial Severity Level	8
5.4.2	Downgrade of Service Request Levels	9
5.4.3	Upgrade of Service Request Levels	9
5.4.4	Adherence to Severity Levels definitions	9
5.5	Service Request Escalation	9
6	Oracle Cloud Suspension and Termination Policy	9
6.1	Termination of Cloud Services	9
6.2	Termination of Pilot Environments	10
6.3	Suspension Due to Violation	10



Overview

These Oracle Cloud Hosting and Delivery Policies (the "Delivery Policies") describe the Oracle Cloud Services ordered by You. These Delivery Policies may reference other Oracle Cloud policy documents; any reference to "Customer" in these Delivery Policies or in such other policy documents shall be deemed to refer to "You" as defined in the ordering document. Capitalized terms that are not otherwise defined in this document shall have the meaning ascribed to them in the Oracle agreement, ordering document or policy.

Your ordering document or Oracle's Service Specifications (such as Cloud Service Pillar documentation or Service Descriptions) may include additional details or exceptions related to specific Oracle Cloud Services. The Cloud Service Pillar documentation, the Service Descriptions and the Program Documentation for Oracle Cloud Services are available at <http://www.oracle.com/contracts>.

Oracle Cloud Services are provided under the terms of the Oracle agreement, ordering document and Service Specifications applicable to such services. Oracle's delivery of the Services is conditioned on Your and Your users' compliance with Your obligations and responsibilities defined in such documents and incorporated policies. These Delivery Policies, and the documents referenced herein, are subject to change at Oracle's discretion; however Oracle policy changes will not result in a material reduction in the level of performance, security, or availability of the Cloud Services provided during the Services Period of Your order.

Oracle Cloud Services are deployed at data centers or third-party infrastructure service providers retained by Oracle, with the exception of Oracle Remote Cloud Services. Oracle Remote Cloud Services are Public Cloud Services that are deployed at Your data center or a third-party data center retained by You. Customers may purchase these services standalone or they may be deployed as the underlying platform for other Oracle Cloud Services. For Oracle Remote Cloud Services, Oracle will deliver to Your data center certain hardware components, including gateway equipment, needed by Oracle to operate these services. You are responsible for providing adequate space, power, and cooling to deploy the Oracle hardware including the gateway, and for ensuring adequate network connectivity for Oracle Cloud Operations to access the Services. Oracle is solely responsible for maintenance of the Oracle hardware components including gateway equipment.

These Delivery Policies do not apply to Oracle BigMachines Express, Oracle ETAWorkforce, or such other Oracle Cloud offerings as specified by Oracle in Your ordering document or the applicable Service Description.


1 Oracle Cloud Security Policy

1.1 Oracle Information Security Practices - General

Oracle has adopted security controls and practices for Oracle Cloud Services that are designed to protect the confidentiality, integrity, and availability of customer data that is hosted by Oracle in the Services. Oracle continually works to strengthen and improve those security controls and practices.

Oracle Cloud Services operates under practices which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected.

Oracle Cloud information security practices establish and govern areas of security applicable to Oracle Cloud Services and to Your use of such Services. Oracle personnel (including employees, contractors, and temporary employees) are subject to the Oracle information security practices and any additional policies that govern their employment or the Services they provide to Oracle.



Rather than focusing on individual components, Oracle Cloud takes a holistic approach to information security, implementing a multilayered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

1.2 User Encryption for External Connections

Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a TLS enabled connection, that connection is negotiated for at least 128 bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each version of Cloud Services will be made available via a portal accessible to You or in the corresponding Service Description. In some cases, a third party site that You wish to integrate with the Cloud Service may not accept an encrypted connection. For Cloud Services where HTTP connections with the third party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.3 Physical Security Safeguards

Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Oracle controlled co-locations/datacenters currently include for example:

- » Physical access requires authorization and is monitored.
- » All employees and visitors must visibly wear official identification while onsite.
- » Visitors must sign a visitor's register and be escorted and/or observed while onsite.
- » Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards.

Additional physical security safeguards are in place for Oracle controlled Cloud data centers, which currently include safeguards such as:

- » Premises are monitored by CCTV.
- » Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles.
- » Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management.

This section does not apply to Oracle Remote Cloud Services. You must provide secured computing facilities for the hosting and operation of the Service related hardware, including the gateway hardware required for Oracle to access the Services.

1.4 Oracle Software Security Assurance

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products and services, including the Oracle Cloud Services. The OSSA program is described at <http://www.oracle.com/us/support/assurance/overview/index.html>.

1.5 Customer Security Related Obligations

You are responsible for:

- » Implementing Your own comprehensive system of security and operational policies, standards and procedures, according to Your risk-based assessments and business requirements.
- » Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to the Services.



- » Managing client device security controls, so that antivirus and malware checks are performed on data or files before importing or uploading data into the Services.
- » Maintaining Customer-managed accounts according to Your policies and security best practices.
- » Additionally, for Oracle Remote Cloud Services, You are responsible for providing adequate network security (e.g., intrusion detection systems, access controls, and firewalls) to prevent unauthorized access to your Oracle Cloud Service from your networks.

2 Oracle Cloud Service Continuity Policy

2.1 Oracle Cloud Services High Availability Strategy

Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers including network infrastructure, program servers, database servers, and/or storage.

2.2 Oracle Cloud Services Backup Strategy

Oracle periodically makes backups of Your production data in the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services, and may also be stored at an alternate location for retention purposes. A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. Oracle typically does not update, insert, delete or restore Your data on Your behalf. However, on an exception basis and subject to written approval and additional fees, Oracle may assist You to restore data which You may have lost as a result of Your own actions.

3 Oracle Cloud Service Level Objective Policy

3.1 Hours of Operation

The Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth in the agreement, the ordering document and this *Oracle Cloud Service Level Objective Policy*.


3.2 Service Availability

Commencing at Oracle's activation of Your production service, Oracle works to meet the Target Service Availability Level, or Target Uptime, of 99.5% in accordance with the terms set forth in the Cloud Service Pillar documentation for the applicable Cloud Service (or such other Target System Availability Level or Target Uptime specified by Oracle for the Cloud Service in such documentation).

The foregoing is contingent on Your adherence to Oracle's recommended minimum technical configuration requirements for accessing and using the Services from Your network infrastructure and Your user work stations as set forth in the Cloud Services Program Documentation.

3.2.1 Measurement of Availability

Following the end of each calendar month of the Services Period, Oracle measures the System Availability Level or System Uptime over the immediately preceding month by dividing the difference between the total number of



minutes in the monthly measurement period and any Unplanned Downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

3.2.2 Reporting of Availability

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

3.3 Definition of Unplanned Downtime


"Unplanned Downtime" means any time during which the Services are not Available, but does not include any time during which the Services or any Services component are not Available due to:

- » A failure or degradation of performance or malfunction resulting from scripts, data, applications, equipment, infrastructure, software, performance testing or monitoring agents directed or provided or performed by You;
- » Outages caused by scheduled and announced maintenance, or outages initiated by Oracle at Your request or direction or initiated by You for maintenance, activation of configurations, backups or other purposes that require the Services to be temporarily taken offline;
- » Unavailability of management, auxiliary or administration services, including administration tools, reporting services, utilities, third party software components, or other services supporting core transaction processing, not within the sole control of Oracle;
- » Outages resulting from Your equipment, third party equipment or software components not within the sole control of Oracle;
- » For Oracle Remote Cloud Services, downtime or other unavailability, including due to maintenance, of Your data center;
- » For Oracle Remote Cloud Services, downtime or other unavailability occurring outside the on-site hours defined under Your order for Oracle's Cloud Operations personnel at Your data center;
- » Events resulting from an interruption or shut down of the Services due to circumstances reasonably believed by Oracle to be a significant threat to the normal operation of the Services, the operating infrastructure, the facility from which the Services are provided, access to, or the integrity of Your Content (e.g., a hacker or malware attack);
- » Outages due to system administration, commands, or file transfers performed by Your users or representatives;
- » Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and Oracle's other vendors), or other force majeure events or circumstances outside of Oracle's control;
- » Inability to access the Services or outages caused by Your conduct, including Your negligence or breach of Your contractual obligations;
- » Your lack of availability or unreasonable delay in responding to incidents that require Your participation for source identification and/or resolution, including meeting Your responsibilities for any Services; or
- » Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to Your conduct or circumstances outside of Oracle's control.

Oracle Cloud Services are "not available" at any time during which a problem with the service prevents Your connectivity to the service as applicable in the corresponding pillar documentation

3.4 Monitoring

Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud production service as applicable and the operation of infrastructure and network components. Oracle does not monitor, or



address deviations experienced by any non-Oracle managed components used by You in the Services, such as non-Oracle applications.

3.4.1 Monitored Components

Oracle monitors the hardware that supports the Oracle Cloud Services, and currently generates alerts for monitored network components, such as CPU, memory, storage, database, and other components. Oracle's Operations staff monitors alerts associated with deviations to Oracle defined thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

3.4.2 Customer Monitoring & Testing Tools

Due to potential adverse impact on service performance, security and availability, You may not, as to any program or feature of, or service component within, the Services, (a) use Your own testing tools (including automated user interfaces and web service calls to any Oracle Cloud Service) or perform network or vulnerability scans or penetration tests to directly or indirectly seek to measure security, or (b) use Your own monitoring tools (including automated user interfaces and web service calls to any Oracle Cloud Service) to directly or indirectly seek to measure availability or performance.

You may not use nor authorize the use of data scraping tools or technologies to collect data available through any Oracle user interface or via web service calls without the express written permission of Oracle. Oracle reserves the right to require Your proposed data scraping tools to be validated and tested by Oracle prior to use in production and to be subsequently validated and tested annually. Oracle may require that a written statement of work be executed to perform such testing and validation work subject to additional fees.

You may not make workload changes beyond the amount permitted under the entitlements provided under Your order.

Oracle reserves the right to remove or disable access to any tools or technologies that violate the restrictions in this section, without any liability to You.

4 Oracle Cloud Change Management Policy

4.1 Oracle Cloud Change Management and Maintenance


Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software that is provided by Oracle as part of the Services, to maintain operational stability, availability, security, performance, and currency of the Oracle Cloud. Oracle follows formal change management procedures to review, test, and approve changes prior to application in the production service.

Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer specific changes. Oracle Cloud change management procedures are designed to minimize service interruption during the implementation of changes.

Oracle reserves specific maintenance periods for changes that may require the Services to be unavailable during the maintenance period. Oracle works to ensure that change management procedures are conducted during scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements.

Oracle will provide prior notice of modifications to the standard maintenance period schedule. For Customer-specific changes and upgrades, where feasible, Oracle will coordinate the maintenance periods with You.

For changes that are expected to cause service interruption, Oracle will work to provide prior notice of the anticipated impact. The durations of the maintenance periods for planned maintenance are not included in the



calculation of Unplanned Downtime minutes in the monthly measurement period for System Availability Level (see the *Oracle Cloud Service Level Objective Policy*). Oracle uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that cause service interruptions.

4.1.1 Emergency Maintenance

Oracle may be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the Services. Emergency maintenance may include program patching and/or core system maintenance as required. Oracle works to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances as determined by Oracle, will work to provide 24 hours prior notice for any emergency maintenance requiring a service interruption.

4.1.2 Major Maintenance Changes

To help ensure continuous stability, availability, security and performance of the Cloud Services, Oracle reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control, typically no more than twice per calendar year. Each such major change event is considered scheduled maintenance and may cause the Cloud Services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. Oracle will work to provide no less than 60 days prior notice of a major change event.

4.1.3 Data Center Migrations

Oracle may migrate Your Services deployed in datacenters retained by Oracle between production data centers in the same data center region as deemed necessary by Oracle or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days notice to You.

4.2 Software Versioning

4.2.1 Software Upgrades and Updates

Oracle requires all Cloud Services customers to keep the software versions of the Services current with the software versions that Oracle designates as generally available (GA) for such Services. Software updates or upgrades will follow the release of every GA release and are required for the Services in order to maintain version currency. Oracle's obligations under these Delivery Policies, including the *Cloud Service Continuity Policy*, *Cloud Service Levels Objective Policy* and the *Cloud Support Policy*, are dependent on You maintaining GA version currency. Oracle is not responsible for performance, functionality, availability or security issues experienced with Services that may result from running earlier versions.

4.2.2 End of Life

Oracle will not support older versions beyond the End of Life Policy described as follows. Oracle will host and support only the designated GA version of a Service. All other versions of the service are considered as "end of life" (EOL). Oracle does not provide Services for EOL versions. You are required to complete the Services upgrade to the latest version before the EOL of a given version. You acknowledge that failure to complete the upgrade prior to the EOL of a Service version may result in an upgrade automatically performed by Oracle or a suspension of the Services. In certain circumstances where a Service version reaches EOL and Oracle does not make available an upgraded version, Oracle may designate, and require You to transition to, a successor cloud service.

5 Oracle Cloud Support Policy

The support described in this *Oracle Cloud Support Policy* applies only for Oracle Cloud Services and is provided by Oracle as part of such Services under Your order. Oracle may make available, and You may order for additional fees, additional support service offerings made available by Oracle for the Services.

5.1 Oracle Cloud Support Terms

5.1.1 Support fees

The fees paid by You for the Oracle Cloud Services under Your order include the support described in this Oracle Cloud Support Policy. Additional fees are applicable for additional Oracle support services offerings purchased by You.

5.1.2 Support period

Oracle Cloud support becomes available upon the service start date and ends upon the expiration or termination of the Services (the "support period"). Oracle is not obligated to provide the support described in this Oracle Cloud Support Policy beyond the end of the support period.

5.1.3 Technical contacts

Your technical contacts are the sole liaisons between You and Oracle for Oracle Cloud support services. Such technical contacts must have, at minimum, initial basic service training and, as needed, supplemental training appropriate for specific role or implementation phase, specialized service/product usage, and migration. Your technical contacts must be knowledgeable about the Services in order to help resolve system issues and to assist Oracle in analyzing and resolving service requests. When submitting a service request, Your technical contact should have a baseline understanding of the problem being encountered and an ability to reproduce the problem in order to assist Oracle in diagnosing and triaging the problem. To avoid interruptions in support services, You must notify Oracle whenever technical contact responsibilities are transferred to another individual.

5.1.4 Oracle Cloud Support


Support Services for Oracle Cloud consists of:

- » Diagnosis of problems or issues with the Oracle Cloud Services.
- » Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that they perform in all material respects as described in the associated Program Documentation.
- » Support during Change Management activities described in the *Oracle Cloud Change Management Policy*.
- » Assistance with technical service requests 24 hours per day, 7 days a week.
- » 24 x 7 access to a Cloud Customer Support Portal designated by Oracle (e.g., My Oracle Support) and Live Telephone Support to log service requests.
- » Access to community forums.
- » Non-technical Customer service assistance during normal Oracle business hours (8:00 to 17:00) local time.

5.2 Oracle Cloud Customer Support Systems

5.2.1 Cloud Customer Support Portal

Oracle provides customer support for the Cloud Service acquired by You through the Cloud Customer Support Portal designated for that Cloud Service. Access to the applicable Cloud Customer Support Portal is governed by the Terms of Use posted on the designated support web site, which are subject to change. A copy of these terms is available upon request. Access to the Cloud Customer Support Portal is limited to Your designated technical



contacts and other authorized users of the Cloud Services. Where applicable, the Oracle Cloud Customer Support Portal provides support details to Your designated technical contacts to enable use of Oracle Cloud support. All service notifications and alerts relevant to Your Cloud Service are posted on this portal.

5.2.2 Live Telephone Support

Your technical contacts may access live telephone support via the phone numbers and contact information found on Oracle's support web site at <http://www.oracle.com/support/contact.html>.

5.3 Severity Definitions

Service requests for Oracle Cloud Services may be submitted by Your designated technical contacts via the Oracle Cloud Customer Support Portal noted above. The severity level of a service request submitted by You is selected by both You and Oracle, and must be based on the following severity definitions:

Severity 1

Your production use of the Oracle Cloud Services is stopped or so severely impacted that You cannot reasonably continue work. You experience a complete loss of service. The impacted operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- » Data corrupted
- » A critical documented function is not available
- » Service hangs indefinitely, causing unacceptable or indefinite delays for resources or response
- » Service crashes, and crashes repeatedly after restart attempts

Oracle will use reasonable efforts to respond to Severity 1 service requests within fifteen (15) minutes. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, or as long as useful progress can be made. You must provide Oracle with a technical contact during this 24x7 period to assist with data gathering, testing, and applying fixes. You are required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2

You experience a severe loss of service. Important features of the Oracle Cloud Services are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

Severity 3

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Severity 4

You request information, enhancement, or documentation clarification regarding the Oracle Cloud Services, but there is no impact on the operation of such service. You experience no loss of service.

5.4 Change to Service Request Severity Level

5.4.1 Initial Severity Level

At the time Oracle accepts a service request, Oracle will record an initial severity level of the service request based on the above severity definitions. Oracle's initial focus, upon acceptance of a service request, will be to resolve the issues underlying the service request. The severity level of a service request may be adjusted as described below.

5.4.2 Downgrade of Service Request Levels

If, during the service request process, the issue no longer warrants the severity level currently assigned based on its current impact on the production operation of the applicable Oracle Cloud Service, then the severity level will be downgraded to the severity level that most appropriately reflects its current impact.

5.4.3 Upgrade of Service Request Levels

If, during the service request process, the issue warrants the assignment of a higher severity level than that currently assigned based on the current impact on the production operation of the applicable Oracle Cloud Service, then the severity level will be upgraded to the severity level that most appropriately reflects its current impact.

5.4.4 Adherence to Severity Levels definitions

You shall ensure that the assignment and adjustment of any severity level designation is accurate based on the current impact on the production operation of the applicable Oracle Cloud Service. You acknowledge that Oracle is not responsible for any failure to meet performance standards caused by Your misuse or mis-assignment of severity level designations.

5.5 Service Request Escalation

For service requests that are escalated, the Oracle support analyst will engage the Oracle service request escalation manager who will be responsible for managing the escalation. The Oracle service request escalation manager will work with You to develop an action plan and allocate the appropriate Oracle resources. If the issue underlying the service request continues to remain unresolved, You may contact the Oracle service request escalation manager to review the service request and request that it be escalated to the next level within Oracle as required. To facilitate the resolution of an escalated service request, You are required to provide contacts within Your organization that are at the same level as that within Oracle to which the service request has been escalated.

6 Oracle Cloud Suspension and Termination Policy

6.1 Termination of Cloud Services

After termination or expiration of the Services under Your order, or at Your request, Oracle will delete or otherwise render inaccessible the production Services, including Your Content residing therein, in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the service environment.

For a period of no less than 60 days after the termination or expiration of the Services, Oracle will make available Your production data via secured protocols, or keep the service system accessible, for the purpose of data retrieval by You. During this period, the service system should not be used for production activities. Oracle has no obligation to retain Your Content after this 60 day period.

If You need assistance from Oracle to obtain access to or copies of Your Content, You must create a service request in the Cloud Customer Support Portal applicable to the service (e.g., My Oracle Support).

Data retrieval and any related assistance by Oracle is not applicable for Services that do not store Your Content. You are responsible for ensuring that if those Services are dependent on separate Cloud Services, such as Storage Cloud Service or Database Cloud Services, for the storage of data, those separate Cloud Services must have a valid duration through the end of the terminating Service to enable data retrieval.



For Oracle Remote Cloud Services, You must make available for retrieval by Oracle any Service related hardware components, including the gateway, provided by Oracle in good working order and the same condition as at the start of the Services subject to reasonable wear and tear for appropriate use.

6.2 Termination of Pilot Environments

This *Oracle Cloud Suspension and Termination Policy* applies to production pilots of Oracle Cloud Services. Production pilots are not available for all Oracle Cloud Services.

6.3 Suspension Due to Violation


If Oracle detects a violation of, or is contacted about a violation of, Services related terms and conditions or acceptable use policy, Oracle will assign an investigating agent. The investigating agent may take actions including but not limited to suspension of user accounts, suspension of administrator accounts, or suspension of access to the Services until the issues are resolved.



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

 Oracle is committed to developing practices and products that help protect the environment.



EXHIBIT G

ORACLE FUSION SERVICE DESCRIPTIONS

Oracle Fusion Human Capital Management Base Cloud Service-Hosted Employee

Applicable Part # B85800

Users of the Oracle Fusion Human Capital Management Base Cloud Service are authorized to access the following modules or functionalities:

- o Oracle Fusion Global Human Resources
- o Oracle Fusion Network at Work
- o Oracle Fusion Workforce Directory Management
- o Oracle Fusion Benefits
- o Oracle Fusion Absence Management
- o Oracle Fusion Workforce Predictions
- o Oracle Fusion Workforce Modeling Cloud Service
- o Oracle Payroll Interface
- o Oracle Transactional Business Intelligence

Usage Limits: The Oracle Fusion Human Capital Management Base Cloud Service is subject to usage limits based on:

- o A maximum number of Authorized Users (Hosted Employees) as defined in your order
- o Oracle will provision 2 environments for this Oracle Cloud Enterprise Applications. One environment is dedicated for production use and the second environment is dedicated as a stage environment for non-production use. Additional environments may be purchased subject to additional fees.
- o The following usage limits apply per Hosted Employee:

Licensed Metric	Database Storage (Records)	File Storage (MB)	Bandwidth
Hosted Employee (1 Authorized user)	5	200	N/A

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

Oracle Fusion Goal Management Cloud Service-Hosted Named User

Applicable Part #B67291

Users of the Oracle Fusion Goal Management Cloud Service are authorized to access the following module:

- Oracle Fusion Goal Management

Users of Oracle Fusion Goal Management Cloud service are defined as the end users of the actual program as well as your employees, contractors, partners and any other individuals that are managed and/or tracked by this program.

Usage Limits: The Oracle Fusion Goal Management Cloud Service is subject to usage limits based on:

- A maximum number of Authorized Users (Hosted Named User) as defined in your order

- Oracle will provision 2 environments for this Oracle Cloud Enterprise application. One environment is dedicated for production use and the second environment is dedicated as a stage environment for non-production use. Additional environments may be purchased subject to additional fees.
- The following usage limits apply per Hosted Named User:

Licensed Metric	Database Storage (Records)	File Storage (MB)	Bandwidth
Hosted Named User (1 Authorized user)	5	200	N/A

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

Oracle Fusion Performance Management Cloud Service – Hosted Named User:

Applicable Part# B67293

Users of Oracle Fusion Performance Management Cloud Service are authorized to access the following module:

- Oracle Fusion Performance Management

Users of Oracle Fusion Performance Management service are defined as the end users of the actual program as well as your employees, contractors, partners and any other individuals that are managed and/or tracked by this program.

Usage Limits: The Oracle Fusion Performance Management Cloud Service is subject to usage limits based on:

- A maximum number of Authorized Users (Hosted Named User) as defined in your order
- Oracle will provision 2 environments for this Oracle Cloud Enterprise application. One environment is dedicated for production use and the second environment is dedicated as a stage environment for non-production use. Additional environments may be purchased subject to additional fees.
- The following usage limits apply per Hosted Named User:

Licensed Metric	Database Storage (Records)	File Storage (MB)	Bandwidth
Hosted Named User (1 Authorized user)	5	200	N/A

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

Transparent Data Encryption for Oracle Fusion Security Cloud Service - Part #B84494 - Page 138

Oracle Transparent Data Encryption Security Cloud Service – Each

Applicable Part# B84494

Oracle Transparent Data Encryption Security Cloud Service consists of the installation and configuration of the following Oracle database security options:

- Oracle Transparent Date Encryption (TDE)

Usage Limits: The Oracle Transparent Data Encryption Security Cloud Service is subject to usage limits based on:

- Oracle Transparent Data Encryption Security Cloud Service must be purchased for all supported environments under your Cloud Services order. Future expansion of Your Oracle Cloud Services may be subject to additional fees.
- No additional storage is provided. The Oracle Transparent Data Encryption Security Cloud Service uses the storage provided under Your existing Oracle Transparent Data Encryption Security Cloud Service.

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

Oracle Additional Test Environment for Oracle Fusion Cloud Service-Test Environment

Applicable Part #B84490

An Oracle Additional Test Environment provides for the hosting and maintenance of an additional Test Environment, which is a reasonably similar replica of Your Production Service Environment for non-production use such as development, training and testing activities but not for Production operation or stress testing. Certain programs and optional services may not be able to run in the Additional Test Environment. The maintenance or upgrade schedule of the Additional Test Environment is the same as the schedule for Your Stage Service Environment.

Each Additional Test Environment must be contracted for a minimum of twelve (12) months as associated to a new or existing Oracle Cloud Ordering Document. Additional Test Environments will automatically terminate at the end of the Service Period.

Usage Limits: The Additional Test Environment for Oracle Fusion Cloud Services defined above are subject to usage limits based upon:

- A maximum number of two hundred and fifty (250) Authorized Users with no more than twenty (20) concurrent users accessing the system at any one time
- Future expansions of Your Oracle Cloud Services may be subject o additional Fees.

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

EXHIBIT H

ORACLE PAAS AND IAAS – PUBLIC CLOUD DESCRIPTIONS – METERED & NON-METERED

Oracle Data Visualization Cloud Service-Hosted Named User

Applicable Part #: B84522

The Oracle Data Visualization Cloud Service is subject to the following quantities.

Usage Limits:

- A maximum number of Authorized Users (Hosted Named User)
- Each Hosted Named User has entitlement to the Oracle Data Visualization Desktop posted on the Oracle Software Delivery Cloud
- 5 GB of storage for the catalog and snapshots
- 50 GBs of storage for imported data
- Oracle will provision one environment for this Oracle Cloud Service.

Oracle Cloud Policies:

Your order for this Oracle Cloud Service is subject to the *Oracle Cloud Hosting and Delivery Policies*, which may be viewed at www.oracle.com/contracts.

EXHIBIT I

Indemnification and Insurance Requirements (For Information Technology Contracts)

INDEMNIFICATION

Notwithstanding the indemnification in the Agreement, Contractor (also referred hereto as "Mythics") and County of Santa Barbara (also referred hereto as "County," "you," or "your") agree that Mythics shall indemnify County of Santa Barbara for direct damages incurred in connection with the following:

- i. Claims for bodily injury (including death);
- ii. Claims for damage to real or tangible personal property sustained as a result of Mythics or Service Provider ("Oracle") performance of its obligations in the Agreement; or
- iii. Claims, fines and incurred costs relating to Mythics or Oracle's breach of its obligations, including but not limited to Confidentiality, stated in the Agreement.

LIMITATION OF LIABILITY

Notwithstanding the limitation of liability in the Agreement, Mythics and County of Santa Barbara agree that Mythics shall be responsible for direct damages incurred as described in the indemnification offerings and in no event shall exceed, in the aggregate, two (2) times the total amounts actually paid to Mythics for the Oracle Services under your Order in the twelve (12) month period immediately preceding the event giving rise to such claim less any refunds or credits received by Santa Barbara.

NOTIFICATION OF ACCIDENTS AND SURVIVAL OF INDEMNIFICATION PROVISIONS

CONTRACTOR shall notify COUNTY immediately in the event of any accident or injury arising out of or in connection with this Agreement. The indemnification provisions in this Agreement shall survive any expiration or termination of this Agreement.

INSURANCE

CONTRACTOR shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the CONTRACTOR, its agents, representatives, employees or subcontractors.

A. Minimum Scope of Insurance

Coverage shall be at least as broad as:

1. **Commercial General Liability (CGL):** Insurance Services Office (ISO) Form CG 00 01 covering CGL on an "occurrence" basis, including products-completed operations, personal & advertising injury, with limits no less than \$1,000,000 per occurrence and \$2,000,000 in the aggregate.
2. **Automobile Liability:** ISO Form Number CA 00 01 covering any auto (Code 1), or if CONTRACTOR has no owned autos, hired, (Code 8) and non-owned autos (Code 9), with limit no less than \$1,000,000 per accident for bodily injury and property damage.
3. **Workers' Compensation:** as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than \$1,000,000 per accident for bodily injury or disease.
4. **Professional Liability (Errors and Omissions)** Insurance appropriate to the CONTRACTOR'S profession, with limit of no less than \$1,000,000 per occurrence or claim, \$2,000,000 aggregate.
5. **Cyber Liability Insurance:** Cyber Liability Insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as

County of Santa Barbara- Order with Mythics, Inc.

regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

If the CONTRACTOR maintains higher limits than the minimums shown above, the COUNTY requires and shall be entitled to coverage for the higher limits maintained by the CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the COUNTY.

B. Other Insurance Provisions

The insurance policies are to contain, or be endorsed to contain, the following provisions:

1. **Additional Insured** – COUNTY, its officers, officials, employees, agents and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of the CONTRACTOR including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to the CONTRACTOR's insurance at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10 and CG 20 37 if a later edition is used).
2. **Primary Coverage** – For any claims related to this Agreement, the CONTRACTOR's insurance coverage shall be primary insurance as respects the COUNTY, its officers, officials, employees, agents and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, officials, employees, agents or volunteers shall be excess of the CONTRACTOR's insurance and shall not contribute with it.
3. **Notice of Cancellation** – Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the COUNTY.
4. **Waiver of Subrogation Rights** – CONTRACTOR hereby grants to COUNTY a waiver of any right to subrogation which any insurer of said CONTRACTOR may acquire against the COUNTY by virtue of the payment of any loss under such insurance. CONTRACTOR agrees to obtain any endorsement that may be necessary to effect this waiver of subrogation, but this provision applies regardless of whether or not the COUNTY has received a waiver of subrogation endorsement from the insurer.
5. **Deductibles and Self-Insured Retention** – Any deductibles or self-insured retentions must be declared to and approved by the COUNTY. The COUNTY may require the CONTRACTOR to purchase coverage with a lower deductible or retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention.
6. **Acceptability of Insurers** – Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum A.M. Best's Insurance Guide rating of "A- VII".
7. **Verification of Coverage** – CONTRACTOR shall furnish the COUNTY with proof of insurance, original certificates and amendatory endorsements as required by this Agreement. The proof of insurance, certificates and endorsements are to be received and approved by the COUNTY before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the CONTRACTOR's obligation to provide them. The CONTRACTOR shall furnish evidence of renewal of coverage throughout the term of the Agreement. The COUNTY reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.
8. **Failure to Procure Coverage** – In the event that any policy of insurance required under this Agreement does not comply with the requirements, is not procured, or is canceled and not replaced, COUNTY has the right but not the obligation or duty to terminate the Agreement. Maintenance of required insurance coverage is a material element of the Agreement and failure to maintain or renew such coverage or to provide evidence of renewal may be treated by COUNTY as a material breach of contract.
9. **Subcontractors** – CONTRACTOR shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and CONTRACTOR shall ensure that COUNTY is an additional insured on insurance required from subcontractors.
10. **Claims Made Policies** – If any of the required policies provide coverage on a claims-made basis:
 - i. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.

- ii. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of contract work.
- iii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the CONTRACTOR must purchase "extended reporting" coverage for a minimum of five (5) years after completion of contract work.

11. **Special Risks or Circumstances** – COUNTY reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Agreement. CONTRACTOR agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of COUNTY to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of COUNTY.