Privacy Code for Processing Personal Information of Customer Individuals

Introduction

Oracle provides cloud, consulting, technical support and other hosted, remote or on-premises computer-based information technology services to its Customers which may involve access to or storage of Personal Information of **Customer Individuals**. Oracle processes such Personal Information as a Processor on behalf of its Customers.

The Oracle Code of Ethics and Business Conduct expresses Oracle's commitment to conduct our business in accordance with high ethical standards and in accordance with applicable laws and Oracle policies, including the protection of Personal Information. This Privacy Code for Processing Personal Information of Customer Individuals ("**Processor Code"**) specifies how this commitment shall be implemented with respect to Personal Information.

Article 1 – Scope, Applicability and Implementation

Scope – Oracle as Processor	**1.1**	This Processor Code applies to Personal Information of Customer Individuals subject to EEA Data Protection Laws and Processed by Oracle on behalf of its Customers in its role as a Processor in the course of delivering Services.
Electronic and paper-based Processing	**1.2**	This Processor Code applies to the Processing of Personal Information by Oracle by electronic means and in systematically accessible paper-based filing systems.
Sub-policies and notices	**1.3**	Oracle may supplement this Processor Code through sub-policies and notices that are consistent with this Processor Code.
Compliance Responsibility	**1.4**	This Processor Code is binding on Oracle. The Responsible Line of Business Executive shall be accountable for his/her business organization's compliance with this Processor Code. Oracle Staff must comply with this Processor Code.
Effective date	**1.5**	This Processor Code enters into force as of June 26, 2019. The Processor Code (including a list of the Group Companies that may be involved in Processing of Personal Information,) will be published on the Oracle Internet site.

Processor Code supplements prior policies **1.6** This Processor Code supplements all Oracle privacy policies that exist on the Effective Date.

Implementation **1.7** This Processor Code shall be implemented within Oracle based on the timeframes specified in Article 15.

Role of Oracle EMEA **1.8** Oracle Corporation has tasked Oracle EMEA with the coordination and implementation of this Processor Code.

Advice Privacy Professional **1.9** Where there is a question as to the applicability of this Processor Code, Staff shall seek the advice of the appropriate Privacy Professional prior to the relevant Processing.

Article 2 – Services Contract

Services Contract **2.1** Oracle shall Process Personal Information only on the basis of a validly entered into written or electronic services contract with a Customer (**Services Contract**), which complies with EEA Data Protection Law

The Oracle Contracting Entity may use Sub-processors, both Oracle Sub-Processors and Third Party Sub-processors, in the regular performance of Services Contracts. The Services Contract shall authorize the use of such Sub-processors, provided that the Oracle Contracting Entity remains liable to the Customer for the performance of the Services Contract by the Sub-processors in accordance with the terms of the Services Contract. Article 7 shall apply if the Services Contract explicitly authorizes the use of Third Party Sub-processors.

Termination of the Services Contract **2.2** Upon termination of the Services Contract, Oracle shall fulfill its obligations to the Customer in the Services Contract with regard to:

(i) returning Personal Information, including by providing data retrieval functionality (such as the ability to download Personal Information) where available for the relevant Services; or
(ii) promptly deleting any remaining copies of Personal Information in accordance with the Services Contract and, upon the Customer's request, confirm that it has done so.

Audit of termination measures

2.3 Upon termination, Oracle shall, at the request of the Customer, allow for its Processing facilities to be audited in accordance with Articles 10.2, 10.3 and 10.4 (as applicable) to verify that Oracle has complied with its obligations under Article 2.2.

Article 3 – Compliance obligations Oracle

Instructions of the Controller

3.1 Oracle shall Process Personal Information only on behalf of the Customer and in accordance with any instructions received from the Customer consistent with the terms of the Services Contract.

Compliance with Applicable Law

3.2 Oracle shall Process Personal Information only in accordance with the Applicable Processor Law and shall deal promptly and appropriately with requests for assistance of the Customer as reasonably required to ensure compliance of the Processing of Personal Information with its obligations under the Applicable Controller Law in accordance with the Services Contract.

Notification of non-compliance, substantial adverse effect

3.3 If Oracle:

(i) determines that it is unable for any reason to comply with its obligations under Articles 3.1 and 3.2 and Oracle cannot cure this inability to comply; or

(ii) becomes aware of any circumstance or change in the Applicable Processor Law, except with respect to the Mandatory Requirements, or an instruction of the Customer, that is likely to have a substantial adverse effect on Oracle's ability to meet its obligations under Articles 3.1, 3.2 or 10.2;

Oracle shall promptly notify Oracle EMEA and the Customer thereof, in which case the Customer will have the right to temporarily suspend the relevant Service(s) under this Processor Code to Oracle until such time the Processing is adjusted in such a manner that the non-compliance is remedied. To the extent such adjustment is not possible, the Customer shall have the right to terminate the relevant Service(s) in accordance with the terms of the Services Contract.

Request for disclosure of Personal Information

3.4 If Oracle receives a request for disclosure of Personal Information from a law enforcement authority, state security body or other governmental authority (**Authority**), it will first assess on a case-by-case basis whether this request

(**Disclosure Request**) is legally valid and binding on Oracle. Any Disclosure Request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law.

Subject to the following paragraph, Oracle shall promptly inform the Customer, the Lead SA and the Customer SA of any legally valid and binding Disclosure Requests, and will request the Authority to put such Disclosure Requests on hold for a reasonable delay in order to enable the Lead SA to issue an opinion on the validity of the relevant disclosure.

If the suspension and/or notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Oracle will request the Authority to waive this prohibition and will document that it has made this request. In any event, Oracle will on an annual basis provide to the Lead SA general information on the number and type of Disclosure Requests it received in the preceding 12-month period.

Inquiries of the Customer

3.5 Oracle shall deal promptly and appropriately with inquiries of the Customer related to the Processing of the Personal Information pursuant to the terms of the Services Contract.

Article 4 – Processor purposes and Description of Processing

Processor Purposes

4.1 As a Processor, Oracle may Process Personal Information for one or more of the following purposes**:**

(i) the provision of Oracle cloud services including:

(a) hosting, storage, backup, or archiving;

(b) maintenance and performance of systems and IT infrastructure (e.g., auditing use, managing servers);

(c) IT security purposes, including system resiliency and incident management;

(d) backup and disaster recovery;

(e) service change management;

(ii) the provision of Oracle technical support services including:

(a) providing technical assistance and product updates to Customers with regard to Oracle products, systems and

services;

(b) life-cycle management of Oracle products, systems and services (e.g., planning, evaluation, demonstration, installation, calibration, maintenance, decommissioning) to facilitate continued and sustained use by a Customer of Oracle products, systems and services.

(iii) the provision of Oracle consulting services and advanced customer support services including:

(a) development and architecture services for the purpose of adjusting Oracle products, systems or services to meet a Customer's specifications (e.g., by engaging application specialists, undertaking project management activities, modifying of device or system);

(b) migration, implementation, configuration, consolidation, performance testing and tuning services;

(c) customer on-site support services for specific projects or on an ongoing basis;

(d) personalized and priority technical support services for critical customer systems and applications.

(iv) Oracle internal business and services process execution and management, including operation of the systems and networks these services run on, and which may involve incidental Processing of Personal Information for:

(a) internal auditing of Oracle Processor-related activities;

(b) activities related to compliance with applicable law or regulation (e.g., data processing law);

(c) use of de-identified, aggregate data to facilitate continuity, sustainability, service analysis and improvement of Oracle products and services.

Description of Processing

4.2 Depending on the relevant Services, Oracle may Process some or all of the following categories of Personal Information:

(i) personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords;

(ii) 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;
(iii) employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details;
(iv) financial details; goods and services provided;
(v) unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

Oracle may Process Personal Information related to some or all of the following categories of Customer Individuals:

(i) Customer representatives
(ii) Customer end users
(iii) Customer employees
(iv) Customer job applicants
(v) Customer contractors or partners
(vi) Customerend-customers and consumers

Article 5 – Security Requirements

Data security 5.1 Oracle has implemented and will maintain appropriate technical, physical and organizational measures. These measures take into account the nature, scope and purposes of Processing as specified in this Processor Code and are designed to protect Personal Information from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing. Oracle shall in any event implement and maintain the Corporate Security Pratices specified in Annex 2 of this Processor Code, which may be revised by Oracle, provided that such changes do not in any material manner diminish the level of security provided for under this Processor Code.

Data access and confidentiality **5.2** Oracle shall provide Oracle Staff access to Personal Information only to the extent necessary to perform the Processing. Oracle shall impose confidentiality obligations on Staff that has access to Personal Information.

Reporting of unauthorized access Processing **5.3** Where Oracle Global Information Security becomes aware and determines that Personal Information has been subject to unauthorized Processing (including by an Oracle employee) that compromises the confidentiality, integrity or availability of such Personal Information ("**Personal Information Breach**"), Oracle will report such Personal Information Breach without undue delay to the Customer to the extent permitted by applicable law. Additional details regarding the reporting process and details regarding the Personal Information Breach are specified in the Services Contract.

Article 6 – Transparency to Customer Individuals

Other Requests of Customer Individuals **6.1** Oracle shall promptly notify the Customer of requests or complaints that are received directly from a Customer Individual without responding to such requests or complaints. If Oracle receives such a request or complaint from a Customer Individual, Oracle will refer the Customer Individual to the Customer to address the request or complaint.

Article 7 – Third Party Sub-processors

Third Party Sub-processing Contracts **7.1** Third Party Sub-processors may Process Personal Information only if the Third Party Sub-processor has a binding contract with Oracle. The contract shall impose the same level of data protection and security-related Processing terms on the Third Party Sub-processor as those imposed on the Oracle Contracting Entity by the Services Contract and this Processor Code.

Publication of Lists of Third Party Sub-processors **7.2** Oracle shall publish and maintain on the appropriate Oracle website or online support portal lists of the Third Party Sub-processors involved in the performance of the relevant Services. This overview shall be regularly updated to reflect changes.

Notification new Third Party Sub-processors and right to object

7.3 Oracle shall provide the option to Customers to be notified of any intended changes to the lists of Third Party Sub-processors engaged by Oracle for the delivery of the Services. Within fourteen calendar days of the Customer receiving such notice, the Customer may object to the involvement of such Third Party Sub-processor in the delivery of the Services, providing objective justifiable grounds related to the ability of such Third Party Sub-processor to protect Personal Information or comply with applicable data protection or security requirements. In the event the objection is not unreasonable, Oracle and the Customer will work together in good faith to find a solution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Sub-processors' compliance or making the Services available without the involvement of such Third Party Sub-processor. To the extent the parties cannot reach a mutually acceptable solution within a reasonable timeframe, the Customer shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to Oracle or the Customer and (iii) without relieving the Customer from its payment obligations under the Services Contract up to the date of termination. If the termination in accordance with this Section 7.3 only pertains to a portion of the Services under a Services Contract, Oracle and Customer will enter into an amendment or replacement contract to reflect such partial termination.

Article 8 – Supervision and compliance

Global Data Protection Officer

8.1 Oracle Corporation has appointed a Global Data Protection Officer who is responsible for:

(i) developing, reviewing and updating Oracle's privacy policies, procedures, system information and training an awareness programs (as required by Article 9);

(ii) supervising and ensuring compliance with this Processor Code;

(iii) providing the annual report (as required by Article 10.5) and periodic reports, as appropriate, to Oracle's General Counsel on data protection risks and compliance issues; overseeing the collection, investigation and resolution of privacy inquiries, concerns and complaints;

(iv) coordinating official investigations or inquiries into the Processing of Personal Information by a public authority;

(v) determining and updating appropriate sanctions for violations of this Processor Code (e.g., disciplinary standards) in co-operation with

other relevant internal functions, such as HR and Legal; and

(vi) Maintaining a fully updated list of the Group Companies and keep track and records of updates to this Processor Code.

Privacy Office

8.2 The Global Data Protection Officer has established and heads Oracle's Privacy Office, consisting of a global network of Privacy Professionals sufficient to direct compliance with this Processor Code within their respective regions or countries.

The Privacy Office performs at least the following tasks:

(i) regularly advising es the global Oracle organization and other relevant internal functions (e.g., Marketing, HR, Development, Sales) on privacy risks and compliance issues;

(ii) ensuring that the Responsible Line of Business Executives maintain an inventory of the system information for all systems and processes that Process Personal Information (as required by article 9.2);

(iii) Implementing the privacy compliance framework (as developed by the Privacy Office in accordance with Article 9);

(iv) making itself available for requests for privacy approvals or advice;

(v) handling privacy requests and complaints;

(vi) owning and authorizing all appropriate privacy sub-policies in their regions or countries; and

(vii) cooperating with the relevant internal functions, including legal, information security, operations and development.

Responsible Line of Business Executive

8.3 The Responsible Line of Business Executive shall perform at least the following tasks:

(i) ensuring that the policies and procedures are implemented and the system information is maintained (as required by Article 9);

(ii) maintaining (or ensuring access to) an inventory of the system information for all systems and processes that Process Personal Information and providing such system information to the Privacy Office as required for the Privacy Office to comply with task listed in Article 8.3 sub (ii);

(iii) ensuring that Personal Information is returned or securely deleted upon termination of the Services Contract (as required by Article 2.2);

(iv) consulting with the Privacy Office whenever there is a conflict between

the Processor Code and applicable law (as required by Article 13.1);

(v) informing the Privacy Office of any new legal requirement that the Responsible Line of Business Executive believes to interfere with Oracle's ability to comply with this Processor Code (as required by Article 13.2).

Privacy Professionals with statutory position

8.4 Where a Privacy Professional holds his/her position pursuant to law, he/she shall carry out his/her job responsibilities to the extent they do not conflict with his/her statutory position.

Article 9 – Policies, procedures and training

Policies and procedures

9.1 Oracle shall develop and implement policies and procedures to comply with this Processor Code.

System information

9.2 Oracle shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Information (e.g., inventory of systems and processes, privacy impact assessments). A copy of this information will be provided to the Lead SA or to a Customer SA upon request.

Staff training

9.3 Oracle shall provide training on the obligations and principles laid down in this Processor Code and other privacy and data security obligations to Staff that has access to, handles, or has responsibilities associated with managing Personal Information.

Article 10 – Monitoring compliance

Internal audits

10.1 Oracle's Business Assessment and Audit (BA&A) organization shall audit business processes and procedures that involve the Processing of Personal Information for compliance with this Processor Code, including methods of ensuring that corrective actions will take place. The audits shall be carried out in the course of the regular activities of the BA&A organization or at the request of the Global Data Protection Officer or the General Counsel. The Global Data Protection Officer may request to have an audit as specified in this Article conducted by an accredited external auditor. Applicable

professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Global Data Protection Officer, the General Counsel and the Privacy Office shall be informed of the results of the audits. Any violations of this Processor Code identified in the audit report will be reported to the Responsible Line of Business Executive. A copy of the audit results related to compliance with this Processor Code will be provided to the Lead SA or the Customer SA upon request.

Customer audit

10.2 Oracle shall, at its option, either:

(i) make the data center facilities or systems it uses for the Processing of Personal Information available for an audit by the Customer or a qualified independent third party auditor selected by the Customer, provided such auditor (a) is reasonably acceptable to Oracle, and (b) has executed a written confidentiality agreement reasonably acceptable to Oracle before conducting the audit. In accordance with the audit provisions of the applicable Services Contract, audits shall be conducted no more than once per year and during regular business hours, and shall be subject to (a) a written request submitted to Oracle at least two weeks in advance of the proposed audit date, (b) a detailed written audit plan reviewed and approved by Oracle and (c) Oracle's on-site health and safety or other relevant security policies. Upon completion of the audit, the Customer shall provide Oracle with a copy of the audit report, which shall be treated as confidential information pursuant to the terms of the Services Contract.

(ii) provide to the Customer a statement issued by a qualified independent third party assessor certifying that the Oracle business processes and procedures that involve the Processing of Personal Information comply with the principles laid down in this Processor Code.

SA audit

10.3 Subject to Article 10.4, the Lead SA may request an audit of the facilities used by Oracle for the Processing of Personal Information for compliance with this Processor Code. In addition, a SA that has the right to audit a Customer (a "**Customer SA**") will be authorized to audit the relevant data transfer for compliance with this Processor Code, subject to the same conditions (regarding the existence of the right to audit, scope, subject and other requirements) as would apply to an audit by that SA of the Customer itself under the Applicable Controller Law.

SA audit procedure

10.4 If a SA requests an audit based on Article 10.3, the following procedure will be followed:

(i) Information sharing: the Customer (or Oracle if the audit is requested by the Lead SA) will attempt to resolve the request using alternative methods of providing information to the SA including Oracle or third party audit or security reports, discussion with Oracle subject matter experts, and review of security, privacy, and operational controls in place. The Customer will have access to its Personal Information in accordance with the Services Contract and may delegate such access to representatives of the SA.

(ii) Examinations: If the SA determines that the information available through these mechanisms is insufficient to address the SA's stated objectives, and upon the Customer's written confirmation that the SA has supervisory authority over the Customer to make such a request, Oracle will provide the SA with the opportunty to communicate with Oracle's auditor at the Customer's expense and if required, a direct right to examine Oracle's data processing facilities used to process the Personal Information on giving reasonable prior notice and during business hours, subject to Oracle's confidentiality policies designed to protect Oracle and other Oracle customer assets.

(iii) Scope: The SA can only access Personal Information belonging to the Customer. The Customer will be liable for Oracle's reasonable additional costs associated with such examination. For clarity, Oracle and its Customers are committed to working together in good faith to resolve a SA request through discussion and interaction among the Customer, Oracle, and the SA.

Annual Report **10.5** The Global Data Protection Officer shall produce an annual Personal Information protection report for the General Counsel on Oracle's compliance with this Processor Code and other relevant issues.

Mitigation **10.6** Oracle shall, if so indicated, ensure that adequate steps are taken to address breaches of this Processor Code identified during the monitoring or auditing of compliance pursuant to this Article 10.

Article 11 – Legal issues

Rights of Customer Individuals **11.1** If Oracle violates the Processor Code with respect to Personal Information of a Customers Individual (**Affected Individual**) and the Affected Individual has a claim against the Customer under Applicable Controller Law with re-

spect to such violation but is unable to enforce the claim against the Customer because: (i) the Customer has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the legal obligations of the Customer by contract or by operation of law (in which case the Affected Individual should enforce its rights against such successor entity), the Affected Individual can enforce as third party beneficiary against the Oracle Contracting Entity any claim as a result of Oracle's breach of Articles 1.5, 2.1, 2.2, 3, 5, 6.1, 7.1, 7.3, 10.2, 10.3, 11.1, 11.2, 11.3, 11.4, 11.7, 11.8 and 13.3.[1]

To the extent the Affected Individual may enforce any such rights against the Oracle Contracting Entity, the Oracle Contracting Entity may not rely on a breach by a Subprocessor of its obligations to avoid liability except to the extent any defense of Subprocessor would also constitute a defense of Oracle. Oracle may, however, assert any defenses or rights that would have been available to the Customer. Oracle also may assert any defenses that Oracle could have asserted against the Customer (such as contributory negligence) in defending against the Affected Individual's claim.

Complaints Procedure

11.2 Affected Individuals may file a written (including by email) complaint in respect of any claim they have under Article 11.1 with the Privacy Office. Affected Individuals may also file a complaint or claim with the SAs or the courts in accordance with Article 11.3.

The Privacy Office shall be responsible for handling such complaints. Each complaint will be assigned to an appropriate Staff member (either within the Privacy Office or within the applicable business unit or functional area). The appropriate Staff member will:

(i) Promptly acknowledge receipt of the complaint;

(ii) Analyze the complaint and, if needed, initiate an investigation;

(iii) If the complaint is well-founded, advise the applicable Privacy Professional so that a remediation plan can be developed and executed; and

(iv) Maintain records of all complaints received, responses given, and remedial actions taken by Oracle.

Oracle will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Affected Individual within one calandar month of receipt of the complaint. The response will be in writing and will be sent to the Affected Individual via the means that the Affected

[1] Substantially revised due to WP257

Individual originally used to contact Oracle (e.g., via mail or email). The response will outline the steps that Oracle has taken to investigate the complaint and will indicate Oracle's decision regarding what steps (if any) it will take in response to the complaint.

In the event that Oracle cannot reasonably complete its investigation and response within one calandar month, it shall inform the Affected Individual within one calendar month of receipt of the compliant that the investigation is ongoing and that a response will be provided within the next two calandar months starting at the end of the first calendar month.

If Oracle's response to the complaint is unsatisfactory to the Affected Individual (e.g., the request is denied without providing an adequate justification) or Oracle does not observe the conditions of the complaints procedure set out in this Article 11.2, the Affected Individual can file a complaint or claim with the authorities or the courts in accordance with Article 11.3.

Jurisdiction for Claims of Customer Individuals

11.3 The Affected Individual may, at his/her choice, submit any claim under Article 11.1 to against the Oracle Contracting Entity:

(i) the Lead SA or the competent courts in Ireland, against Oracle EMEA; or

(ii) the SA in the country of his/her habitual residence, place of work or place where the infringement took place against the Oracle Contracting Entity; or

(iii) the courts in the country of his/her habitual residence, or the country of origin of the data transfer under this Processor Code, against the Oracle Contracting Entity.

The courts and SAs shall apply their own substantive and procedural laws to the dispute. Any choice made by the Affected Individual will not prejudice the substantive or procedural rights he or she may have under applicable law.

Available remedies, limitation of damages, burden of proof re. damages for Customer Individuals

11.4 In case an Affected Individual has a claim under Article 11.1, such Affected Individuals shall be entitled to compensation of actual direct damages. However, the Oracle Contracting Entity or Oracle EMEA shall be liable only for actual direct damages (which exclude, without limitation, any indirect, incidental, special, punitive or consequential damages or any lost profits or revenue, lost turnover, cost of capital, downtime cost, and loss of data) suffered by an Affected Individual resulting from a violation of this Processor Code.

Regarding the burden of proof in respect of such damages, it will be for the

Affected Individual to demonstrate that he/she has suffered actual direct damages and to establish facts which show that the damage has occurred because of a violation of this Processor Code. It will subsequently be for the Oracle Contracting Entity or Oracle EMEA to prove that the damages suffered by the Affected Individual due to a violation of this Processor Code are not attributable to a Group Company or a Subprocessor or to assert other applicable defenses.

Rights of Customers

11.5 The Customer may enforce this Processor Code against the Oracle Contracting Entity or, if the Oracle Contracting Entity is not established in an EEA Country, against Oracle EMEA. Oracle EMEA shall ensure that adequate steps are taken to address violations of this Processor Code by the Oracle Contracting Entity or any other Group Company.

The Oracle Contracting Entity or Oracle EMEA may not rely on a breach by another Group Company or a Subprocessor of its obligations to avoid liability.

Available remedies, limitation of damages, burden of proof re. damages for Customers

11.6 In case of a violation of this Processor Code, Customers shall be entitled to compensation of damages consistent with the Services Contract.

Mutual assistance Group Companies and redress

11.7 All Group Companies shall cooperate and assist each other to the extent reasonably possible to achieve compliance with this Processor Code, including an audit or inquiry by the Customer or a SA competent for Customer.

The Oracle Group Company receiving a request for information pursuant to Article 6.1 or a claim pursuant to Article 11.1, is responsible for promptly informing the Privacy Office thereof and handling any communication with the Customer Individual regarding his request or claim as instructed by the Privacy Office.

The Oracle Group Company that is responsible for the Processing to which the request or claim relates, shall bear all costs involved and reimburse any costs made by other Oracle Group Companies in respect thereof upon request.

Advice by Lead SA, decisions other

11.8 Oracle shall abide by the advice of the Lead SA issued on interpretation and application of this Processor Code. Oracle shall abide by a binding decision

Data Protection Authorities of the SA competent for the Customer as instructed by Customer in accordance with Articles 3.2 and 3.3.

Article 12 – Sanctions for non-compliance

Non-compliance **12.1** Non-compliance of Oracle employees with this Processor Code may result in disciplinary action in accordance with Oracle policies and local law, up to and including termination of employment.

Article 13 – Conflicts between this Processor Code and Applicable Processor Law

Conflict between Processor Code and law **13.1** Where there is a conflict between Applicable Processor Law and this Processor Code, the relevant Responsible Line of Business Executive shall consult with the Privacy Office to determine how to comply with this Processor Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal requirements **13.2** The relevant Responsible Line of Business Executive, in consultation with the legal department, shall promptly inform the Privacy Office of any new legal requirement that may interfere with Oracle's ability to comply with this Processor Code.

Reporting to Lead SA and Customer SA **13.3** If Oracle becomes aware that Applicable Processor Law or any change in Applicable Processor Law is likely to have a substantial adverse effect on Oracle's ability to meet its obligations under 3.1, 3.2 or 10.3, Oracle will report this to the Lead SA and the Customer SA.

Article 14 – Changes to this Processor Code

Approval for Changes **14.1** Any changes to this Processor Code require the prior approval of the General Counsel and shall thereafter be communicated to the Group Companies.

Effective Date Of Changes

14.2 Any amendment shall enter into force after it has been approved and made available to Customers on the Oracle Internet site (www.oracle.com).

Prior Versions

14.3 Any request or claim of a Customer Individual involving this Processor Code shall be judged against the version of this Processor Code that is in force at the time the request, complaint or claim is made.

Notification to Lead SA and Customers

14.4 The Global Data Protection Officer shall be responsible for informing the Lead SA of material changes to this Processor Code, if any, on a yearly basis, including a brief explanation of the reasons justifying the update. Where a change to this Processor Code has a significant impact on the Processing conditions of Personal Information, Oracle will promptly inform the Lead SA thereof including a brief explanation for such change as well as provide notice of such change to the Customer. Within 30 days of receiving such notice, the Customer may object to such change by providing written notice to Oracle. In the event that the parties cannot reach a mutually acceptable solution, Oracle shall put in place an alternative data transfer solution. In the event no alternative data transfer solution can be put in place, the Customer will have the right to suspend the relevant transfer of Personal Information to Oracle. In the event a suspension of the relevant data transfers is not possible, Oracle shall enable the Customer to terminate the relevant Customer Services in accordance with the terms of the Services Contract.

Article 15 – Transition Periods

Transition Period for New Group Companies

15.1 Except as otherwise indicated, any entity that becomes a Group Company after the Effective Date shall comply with this Processor Code upon becoming a Group Company.

Transition Period for Divested Entities

15.2 A Divested Entity will remain covered by this Processor Code after its divestment for such period as is required by Oracle to disentangle the Processing of Personal Information relating to such Divested Entity.

Transition Period for IT Systems

15.3 Where implementation of this Processor Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be up to two years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition Period for Existing Agreements

15.4 Where there are existing agreements with Third Parties that are affected by this Processor Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

ANNEX 1: Definitions

Affected Individual	AFFECTED INDIVIDUAL shall mean the individual referred to in Article 11.1
Applicable Controller Law	APPLICABLE CONTROLLER LAW shall mean the Data Protection Laws of the EEA Countries that are applicable to the Customer as the Controller of Personal Information.
Applicable Processor Law	APPLICABLE PROCESSOR LAW shall mean the Data Protection Laws that are applicable to Oracle as the Processor of Personal Information.
Global Data Protection Officer	GLOBAL DATA PROTECTION OFFICER shall mean the officer referred to in Article 8.1
Controller	CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Information.
Customer	CUSTOMER shall mean the customer who has entered into a contract with Oracle for the delivery of Oracle Services.
Customer SA	CUSTOMER SA shall have the meaning set forth in Article 10.3.
Customer Individual	CUSTOMER INDIVIDUAL shall mean any individual whose Personal Information is Processed by Oracle in its role as a Processor in the course of delivering Oracle Services to a Customer.
Customer Personal Information	CUSTOMER PERSONAL INFORMATION shall mean Personal Information of a Customer Individual.
Data Protection Law	DATA PROTECTION LAW shall mean the laws of a country containing rules for the protection of individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.

Divested Entity	DIVESTED ENTITY shall mean the divestment by Oracle of a Group Company or business by means of: (i) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or (ii) a demerger, sale of assets, or any other manner or form.
EEA Countries	EEA COUNTRIES (European Economic Area Countries) shall mean all Member States of the European Union, Norway, and for purposes of this Processor Code, Switzerland and the UK post-Brexit.
EEA Data Protection Law	EEA DATA PROTECTION LAW shall mean the data protection laws of the EEA Countries, Switzerland, and (post-Brexit) the United Kingdom.
EEA Data Transfer Restriction	EEA DATA TRANSFER RESTRICTION shall mean any restriction under EEA Data Protection Law regarding outbound transfers of Personal Information.
Effective Date	EFFECTIVE DATE shall mean the date on which this Processor Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean an employee of Oracle.
General Counsel	GENERAL COUNSEL shall mean the General Counsel of Oracle Corporation.
Group Company	GROUP COMPANY shall mean Oracle Corporation and any company or legal entity of which Oracle Corporation, directly or indirectly owns more than 50% of the issued share capital.
Lead SASA	LEAD SASA shall mean the supervisory authority of Ireland.

Mandatory Requirements	MANDATORY REQUIREMENTS shall mean mandatory requirements of Applicable Processor Law which do not go beyond what is necessary in a democratic society i.e. which constitute a necessary measure to safeguard national security defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the state or the protection of a Customer Individual or the rights and freedoms of others.
Oracle	ORACLE shall mean Oracle Corporation and its Group Companies.
Oracle Contracting Entity	ORACLE CONTRACTING ENTITY shall mean the Oracle Group Company that has entered into a Services Contract for the provision of Services.
Oracle Corporation	ORACLE CORPORATION shall mean Oracle Corporation, incorporated in the State of Delaware, and having its its principle place of business in the State of California, United States.
Oracle EMEA	ORACLE EMEA shall mean Oracle EMEA Limited, having its registered seat in Dublin, Ireland.
Oracle Sub-processor	ORACLE SUB-PROCESSOR shall mean any Group Company engaged by Oracle as a Sub-processor.
Personal Information	PERSONAL INFORMATION shall mean any information relating to an identified or identifiable individual.
Privacy Professional	PRIVACY PROFESSIONAL shall mean the privacy professionals appointed by the Global Data Protection Officer pursuant to Article 8.3.
Processing	PROCESSING shall mean any operation that is performed on Personal Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Information.
Processor	PROCESSOR shall mean the entity or natural person which Processes Personal Information on behalf of a Third Party Controller.

Processor Code	PROCESSOR CODE shall mean this f for Processing Personal Information of Customer Individuals.
SA	SA shall mean any supervisory authority of one of the EEA Countries.
Responsible Line of Business Executive	RESPONSIBLE LINE OF BUSINESS EXECUTIVE shall mean the lowest-level Oracle line of business executive or the non-executive general manager of an Oracle ORU (Organizational Reporting Unit) who has primary budgetary ownership of the relevant Processing.
Services	SERVICES shall mean the services listed in Article 4.1 as contracted by the Customer under the Services Contract.
Services Contract	SERVICES CONTRACT shall mean the contract for delivery of Services entered into between an Oracle Group Company and the Customer pursuant to Article 2.1.
Staff	STAFF shall mean all Employees and other persons who Process Personal Information as part of their respective duties or responsibilities, either using Oracle information technology systems or working primarily from Oracle premises.
Sub-processor	SUB-PROCESSOR shall mean any Processor engaged to Process Personal Information as a sub-processor.
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or government authority) outside Oracle or a Customer.
Third Party Sub-processor	THIRD PARTY SUB-PROCESSOR shall mean any Third Party engaged by Oracle as a Sub-processor.
Third Party Sub-processor Contract	THIRD PARTY SUB-PROCESSING CONTRACT shall mean the validly entered into written or electronic agreement between Oracle and the Third party Sub-processor pursuant to Article 7.2.
Interpretations	INTERPRETATION OF THIS PROCESSOR CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in construing any provision of this Processor Code

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning

(iv) the male form shall include the female form

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa

(vi) a reference to a document (including, without limitation, a reference to this Processor Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Processor Code or that other document, and

(vii) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2: Oracle Corporate Security Practices

Oracle Corporate Security Practices

Introduction

The Oracle Corporate Security Practices ("Security Practices") describe the security practices implemented pursuant to Oracle's Corporate security program, and adhered to by Oracle for its operational and services infrastructure under its control, including Oracle's corporate network and systems. As used in this document, "customer data" means any data stored in a customer's computer system (data accessed by or provided to Oracle while performing services for a customer) or customer's Oracle Cloud instance. Third parties engaged by Oracle and that are also provided access to customer data by Oracle ("subprocessors"), will be contractually committed to materially equivalent security practices.

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.

1. Scope

1.1 Overview

The Security Practices are designed to protect the confidentiality, integrity, and availability of both customer and Oracle data. Oracle continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers.

As noted above, this document describes the security practices adhered to by Oracle for its operation and services infrastructure. Companies that Oracle acquires are required to align with these Security Practices as part of the integration process.

Oracle's Cloud, Support, Consulting, and Advanced Customer Support Services lines of business have also developed more detailed statements of security practices that apply to many of their service offerings, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Cloud Hosting & Delivery Policies
- Global Customer Support Security Practices Consulting Security Practices
- Advanced Customer Services Security Practices

2. Oracle Information Security

2.1 Overview

Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle Employees, contingent workers, and sub-processors. They are generally aligned with the ISO/IEC 27002:2013 and 27001:2013 standards, and govern all areas of security within Oracle.

Oracle 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.

2.2 Privacy

The *Oracle Privacy Policy* describes how Oracle collects and uses personal information collected from the Oracle websites that link or refer to the policy as well as from offline sales and marketing activities. It also describes how users can control that collection and use. This policy is available at https://www.oracle.com/legal/privacy/privacy-policy.html.

The *Oracle Services Privacy Policy* describes Oracle's treatment of data that resides on Oracle, customer or third-party systems (including personal information or "PI") to which Oracle may be provided access in connection with the provision of services. This policy is available at https://www.oracle.com/legal/privacy/services-privacy-policy.html.

The *Oracle Marketing Cloud and Oracle Data Cloud Privacy Policy* describes how Oracle Marketing Cloud and Oracle Data Cloud services facilitate the collection and use of information by our customers in connection with interest-based advertising, and is designed to provide tools to help understand and control the collection and use of that information. This policy is available at https://www.oracle.com/legal/privacy/marketing-cloud-data- cloud-privacy-policy.html.

2.3 Enforcement

Oracle requires the reporting of and response to information security incidents in a timely and efficient manner. Oracle also maintains a detailed Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

Oracle's Global Information Security (GIS) organization conducts security reviews, assessments, and audits periodically to confirm compliance with the Oracle information security policies, procedures, and practices.

Where non-compliance is found, GIS works with the relevant Lines of Business to resolve those issues in a timely a manner. GIS reserves the right to intervene as deemed necessary and to isolate environments in non-compliance that put infrastructure or other environments at serious risk.

Oracle employees who fail to comply with Oracle information security policies, procedures, and practices may be subject to disciplinary action, up to and including termination.

3. Organizational Security

Oracle’s overarching Organizational Security is described in the Oracle Security Organization Policy and the Oracle Information Security Policy. The Chief Corporate Architect, who reports directly to the CTO, manages the functional departments directly responsible for identifying and implementing security controls at Oracle. The Global Information Security, Global Product Security, Global Physical Security, and Oracle Security Architecture organizations comprise Oracle Corporate Security, which provides independent security policy, guidance and compliance oversight to Oracle worldwide.

3.1 Oracle Security Oversight Committee

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

3.2 Global Security Organizations

3.2.1 Global Information Security

Global Information Security (GIS) is responsible for security oversight and assurance, policy compliance and enforcement, leading the development of information security policy and strategy, as well as training and awareness at the Corporate level. GIS serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.

3.2.2 Global Product Security

Global Product Security (GPS) acts as a central resource to help Oracle development teams improve the security of Oracle products. GPS’ primary mission is to promote the use of the Oracle Software Security Assurance (OSSA) standards throughout Oracle. Responsibilities include assisting in improving the security of Oracle products in their

development phase, performing security assessments of Oracle products using a variety of techniques, and evaluating potential product security vulnerabilities.

3.2.3 Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of our employees, business enterprise and assets. More information on applicable physical security controls are described in section 6.

3.2.3 Corporate Security Architecture

Corporate Security Architecture (CSA) is responsible for setting Information Security Architecture strategy and direction in support of long-term Corporate objectives and verifying alignment of IT initiatives with Corporate Security Architecture strategy and direction. In addition, CSA identifies and guides IT security infrastructure improvements and reviews security-related technical aspects of IT projects and acts as technical advisor on Corporate Security matters.

3.3 Oracle Information Technology Organizations

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

3.4 Confidentiality Agreements

All Oracle employees and subprocessors who may have access to customer data are subject to a written confidentiality agreement. Prior to performing services for Oracle and prior to accessing any Oracle system or resource, service providers are required to sign a Services Provider Agreement, a Network Access Agreement, and a work order defining the services to be provided.

Oracle is obligated to protect the confidentiality of customer data in accordance with the terms of the Ordering Document, Exhibit, and Statement of Work.

3.5 Independent Review of Information Security

Global Information Security, in conjunction with Oracle Internal Audit, oversees compliance of the security controls, processes, and procedures for Oracle services.

4. Asset Classification and Control

4.1 Responsibility, Inventory, and Ownership of Assets

Overarching controls related to assets are addressed by the *Oracle Information Protection Policy*, the *Oracle Desktop and Laptop Security Policy*, the *Oracle Information Systems Inventory Policy,* and the *Oracle Acceptable Use Policy for Company Resources*. All information assets have an owner who is responsible for the protection and inventory of assets based on the sensitivity and value of information. If ownership has not been assigned, it will default to the administrators of the application or system. This includes maintenance of operations guides and other documentation describing the environments.

4.2 Asset Classification and Control

Oracle provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications in order to provide protection for Oracle and customer information assets. Oracle has defined three classes of confidential information – Internal, Restricted, and Highly Restricted – with each classification requiring corresponding levels of security controls (e.g., encryption requirements for data classified as Restricted or Highly Restricted). Customer data is classified as among Oracle's top two categories of confidential information, which have associated limits on access, distribution and handling. Oracle keeps the information confidential in accordance with the terms of customer's order.

5. Human Resources Security

Oracle places a strong emphasis on personnel security. Measures taken to minimize risks associated with human error, theft, fraud, and misuse of facilities include personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

The *Oracle Code of Ethics and Business Conduct* sets forth Oracle's high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business throughout the world. The standard applies to Oracle employees, contractors, and temporary employees. It covers the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required every two years. The Code of Ethics and Business Conduct is available at the following URL: http://www.oracle.com/us/corporate/investor- relations/cebc-176732.pdf

5.1 Employee Screening

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

5.2 Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters, ad hoc security awareness campaigns, and security related Corporate send mails.

Each employee is required to complete information protection awareness training. The course instructs employees on their obligations under the various Oracle privacy and security policies (such as the *Information Protection Policy*, *Acceptable Use Policy for Company Resources* and the *Services Privacy Policy*). The course also covers data privacy principles and data handling practices that may apply to employees' jobs at Oracle and are required by company policy, including those related to use, access, integrity, sharing, retention, security and disposal of data.

Oracle performs periodic compliance reviews to determine if employees have completed the online awareness-training course. If Oracle determines that an employee has not completed the required course, the employee will be promptly notified and instructed to complete the required training, and may be subject to disciplinary action.

Oracle promotes awareness of, and educates employees about, issues relating to security. Oracle currently prepares and distributes to its employees quarterly newsletters, ad hoc notices and other written material on security. Oracle also may update existing training courses, and develop new courses from time to time, which employees will be directed to complete.

5.3 Enforcement

Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information

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

6. Physical Security

Overarching controls related to physical security are described in the *Oracle Identification and Access Badge Policy*. Oracle Global Physical Security utilize a security risk-based defense in depth or layered methodology designed to balance prevention, detection, protection and response.

Oracle maintains the following physical security standards designed to prohibit unau thorized physical access at all Oracle facilities from which customer data may be handled ("Service Locations"):

- Service Locations have physical access limited to Oracle employees, subcontractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on the premises.
- Visitors to Service Locations are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement.
- Security monitors the possession of keys/access cards and the ability to access the Service Locations. Staff leaving Oracle employment must return keys/cards.

After-hours access to Service Locations is monitored and controlled by Security.

Oracle Physical Security authorizes all repairs and modifications to the security barriers and entry controls at Service Locations owned by Oracle.

7. Communications and Operations Management

Oracle aligns with the IT service management process areas as outlined in the ITIL Infrastructure Library and uses this framework as a guide for operational delivery. Oracle's internal documentation specifies current operational processes and procedures for employees' performance of technical functions.

7.1 Segregation of Duties

Roles within operations are well defined, allowing for segregation of duties. Segregation of duties is achieved by organizing operations into functional groups, where each function is performed by separate groups of employees. Examples of the functional groups include database administrators, System Administrators, and network engineers.

7.2 Protection Against Malicious Code

Oracle's Desktop and Laptop Security Policy requires that all computers connected to Oracle's intranet have anti-virus, firewall and desktop asset management software installed, that all computers that hold Oracle data running a Windows operating system must have Microsoft security updates enabled, and that Oracle personnel install the approved full disk encryption software on their laptops, unless an approved exception has been authorized for appropriate business purposes.

Oracle's Global IT (GIT) organization keeps anti-virus products up-to-date with virus definitions and security updates. GIT is responsible for notifying internal Oracle system users of any credible virus threats and when security updates are available and Oracle employees are required to comply with instructions received through e-mail from the GIT organization. Oracle has also licensed and installed third-party anti-virus and anti-spam products to scan all emails and

attachments (inbound and outbound).

7.3 Network Security Management

Overarching policies related to network infrastructure are described in the *Oracle Network Security Policy* and *Oracle Server Security Policy*. Oracle employs intrusion prevention and detection systems within the Oracle corporate networks to provide surveillance for intercepting and responding to security events as they are identified. Events are analyzed using signature and anomaly detection and Oracle updates the signature database frequently. Alerts are forwarded to Oracle's IT security for review and response to potential threats. Oracle uses router rules, access control and security lists and segmentation on the Oracle network. Oracle's Global IT and Cloud DevOps departments manage and monitor routers and firewall logs and network devices are safeguarded via centralized authentication with audited usage.

7.4 Monitoring and Protection of Audit Log Information

The following sections describe controls utilized by Oracle to monitor and protect audit log information as detailed in the overarching *Oracle Logging and Log Analysis Policy.*

Logging

Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls to protect against operational issues, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.

Log Review

Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security incident management process.

Log Security

Access to logs is provided on the basis of need to know and least privilege. Where feasible, log files are protected by cryptographic hash sum, and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet-accessible.

8. Access Control

Overarching policies for access are described in the *Oracle Logical Access Controls Policy*. Access control refers to the policies, procedures, and tools that govern the access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol.

Oracle uses the principle of "Least privilege" in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.

Oracle uses the principle of "Default deny" that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.

In the event of employee terminations, deaths or resignations, Oracle will take actions to terminate network, telephony and physical access for such former employees. Oracle Corporate Security will periodically review accounts of terminated employees to verify that access has been terminated and that stale accounts are removed from the Oracle network.

8.1 Access Control

The *Oracle Logical Access Control Policy* is applicable to access control decisions for all Oracle employees and any information processing facility for which Oracle has administrative authority. The policy does not apply to publicly accessible internet-facing Oracle systems or customer's end users.

8.2 User Access Management

User Registration

- Access privileges are granted based on job role and require management approval.

Privilege Management

- Authorization is dependent on authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles:
- "Need to know" - Only provide access when required for job function or role
- "Segregation of duties" - Avoid a conflict of interest in the access that is provided
- "Least privilege" - Restricted access to only those resources and information required for a legitimate business purpose

User Password Management

As described in the *Oracle Password Policy*, Oracle enforces strong password policies for Oracle network, operating system, and database accounts in an effort to reduce the chances of intruders gaining access to systems or environments through exploitation of User accounts and their associated passwords.

Review of Access Rights

Network and operating system accounts are reviewed regularly with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to terminate network, telephony, and physical access for such former employees.

Password Use

The use of passwords is addressed in the *Oracle Password Policy.* Oracle employees are obligated to follow rules for password length and complexity, and keep their passwords confidential and secure at all times. Passwords may not be disclosed to any unauthorized person. Under certain circumstances, passwords may be communicated between authorized Oracle employees for the purpose of providing support services.

8.3 Network Access Controls

Network controls implemented for Oracle address the protection and control of customer data during its transmission from one end system to another. The *Oracle Use of Network Services Policy* states that computers, servers, and other data devices connected to the Oracle network must comply with Global IT (GIT) and GIS standards for security, configuration, and access method, in accordance with *Oracle's Acceptable Use Policy for Company Resources.*

9. Information Systems Acquisition, Development, and Maintenance

9.1 Access Control to Program Source Code

Access to Oracle source code is provided on a strict "Need to know" basis to those who require it for an authorized

business purpose.

9.2 Technical Vulnerability Management

Oracle subscribes to vulnerability notification systems to stay apprised of security Incidents, advisories, and other related information. Oracle takes actions on the notification of a threat or risk once it has the opportunity to confirm that both a valid risk exists and that the recommended changes are applicable to the particular system or environment.

10. Information Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to, or handling of, customer data in its possession or under its control, whether the data is held on Oracle hardware assets, those of vendors/suppliers, or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Global Information Security (GIS) organization is required to be informed of such incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those incidents.

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

Oracle will not disclose production data located on Oracle systems, including text and images, except in accordance with your order, your instructions, or to the extent required by law. Oracle will use diligent efforts to inform you, to the extent permitted by law, of any request for such disclosure before disclosure is made.

11. Oracle’s Resilience Management

Oracle has a global Risk Management and Resiliency Program (RMRP), which comprises, among other elements, contingency planning and plan testing designed to enable our critical, internal operations to continue in spite of potentially business-disruptive incidents. The RMRP addresses:

- Personal safety;
- Incident management;
- Business continuity; and
- Technological system recovery.

12. Audit

In the event that the applicable order for services provides you with the right to audit Oracle’s compliance with these security practices, the following procedures apply. You must send Oracle’s Global Information Security organization a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. The parties will work cooperatively to agree on a final audit plan. The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to on-site policies and regulations, and may not unreasonably interfere with business activities. If you would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle. Upon completion of the audit, you will provide Oracle with a copy of the audit report, which is classified as confidential information under the terms of the Agreement. Additional audit terms may be included in your order for services.

13. Customer Data Retention

Except as otherwise specified in an order for services or required by law, upon termination of services or at your request, Oracle will delete your production customer data located on Oracle computers 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 data. For Cloud Services, customer data management is generally "self service" and additional information on features to assist you with data management can be found in the applicable "Service Feature Guidance" document. For other Oracle services, you may consult with your Oracle services contact for additional information on data deletion prior to service completion.

As described in the *Oracle Media Sanitization and Disposal Policy*, media containing Customer Data will be securely sanitized, or destroyed and disposed of when the media is no longer required or able to be used, or the storage media becomes otherwise obsolete. Currently approved sanitization methods are degaussing, shredding, incineration, and verified overwrites of the data. Some hardware such as SSD may include acceptable built-in secure erasure functionality.

14. Reference

As stated above, these security practices should be read in conjunction with any more detailed security practices created by Oracle's Cloud, Global Customer Support, Consulting, and Advanced Customer Services lines of business, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Cloud Hosting & Delivery Policies
- Global Customer Support Security Practices Consulting Security Practices
- Advanced Customer Services Security Practices

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.