OPENAIR SERVICE DATA SECURITY ADDENDUM

For the Cloud Service procured on the applicable Estimate/Order Form (the "OpenAir Service"), Oracle shall maintain commercially reasonable administrative Safeguards designed for the protection, confidentiality, and integrity of Customer Data. All such Safeguards shall be commensurate with the importance of the Customer Data being protected, but in no event less protective than safeguards that Oracle uses to protect its own information or data of similar importance, or as required by applicable law. As of the effective date of the applicable Estimate/Order Form, such Safeguards are described below in this Addendum[1]; provided, however, that Customer acknowledges and agrees that such Safeguards described in this Addendum are not comprehensive and such Safeguards may change during the term of the applicable Estimate/Order Form, as applicable third party security audits, compliance standards and/or certifications evolve/change over time, provided that any such changes to Safeguards will not materially decrease the overall security of the OpenAir Service during the term of the applicable Estimate/Order Form. For the term of the Agreement, Oracle shall comply with all obligations regarding Customer Data under the applicable Estimate/Order Form, including, without limitation, Oracle's obligations to maintain commercially reasonable Safeguards as provided herein.

1. Security Policy. Oracle has, and will maintain, a security policy for its security organization that requires security training and privacy training as part of the training package for Oracle security personnel, as documented in its ISO 27001 certification.
2. Oracle Security Organization. Oracle has, and will continue to have, a dedicated security organization that is responsible for the ongoing monitoring of Oracle's security infrastructure, the review of Oracle products and services, and for responding to Security Incidents.
3. Data Storage and Handling. Storage medium or any equipment with storage capability, including mobile media, used to store Customer Data will be secured and hardened in accordance with industry standard practices. Oracle will maintain a reasonable asset management policy to manage the life cycle (commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of such media. Decommissioned media containing Customer Data will be destroyed in accordance with NIST 800-88 (or similar data destruction standard) at the Moderate level of sensitivity.
4. Data Transmission. Oracle will use strong cryptography and security protocols consistent with industry standards, as documented in the User Guides for the Service.
5. Change Management. Oracle maintains a change management policy to ensure changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.
6. Server Operating Systems. Oracle servers will use a hardened operating system implementation customized for the Service. Oracle will maintain a risk-based prioritized patch management policy.
7. Access Control and Privilege Management. Oracle employs systems and processes to limit physical and logical access based on least privileges and segregation of duties to ensure critical data can only be accessed by authorized Oracle personnel.
8. User Accounts. Customer will have control over the creation, deletion, and suspension of User roles within the Service, as documented in the Service User Guides.
9. Password Policy. As documented in the User Guides for the Service, Customer can apply its own password and authentication policies via the Service's configurable policy settings and when using the single sign on functionality of the Service.
10. Network Connectivity Security Requirements. Oracle will protect its infrastructure with multiple levels of secure network devices.
11. Audits and Certifications. The following security audits and certifications are relevant to the OpenAir Service, as set forth below:
    a. SOC Report Attestations. The American Institute of CPAs (AICPA) has established System and Organization Controls (SOC) frameworks for evaluating and reporting on the effectiveness of a service organization's controls that address specific user needs. With respect to the OpenAir Service, Oracle shall ensure performance of annual third-party attestation reports completed in accordance with the AICPA and IFAC Standards for Assurance Engagements:
        i. Oracle shall ensure performance of an annual SOC 1 / ISAE 3402 Type II report.
        ii. Oracle shall ensure performance of an annual SOC 2 Type II report, for the Security, Availability, and Confidentiality attributes.
        iii. Any material findings that lead to a qualified opinion on the SOC reports will be promptly addressed with the development and implementation of a corrective action plan by Oracle's management.

[1]For clarity, the Safeguards set forth in this Addendum do not apply to any Third-Party Applications and may not apply to optional services subsequently ordered or activated by Customer that are subject to different terms.

b. ISO 27001. ISO 27001 is a leading international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for measuring information security management systems (ISMS). This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS.

   Oracle shall ensure performance of a third-party certification audit of Oracle's ISMS against the requirements of the ISO 27001 standard.

c. No more than once per year, Customer may submit a request for a copy of Oracle's final: a) SOC 1 / ISAE 3402 Type II report; b) SOC 2 Type II report; and (c) ISO 27001 certificate and Statement of Applicability (SOA). Any such reports, certificates and supporting documentation provided by Oracle in connection with this Section are deemed Oracle Confidential Information.

d. If similar third-party audits, standards and/or certifications become available in the future, Oracle may choose to perform such audit and/or certify to such established industry standard selected by Oracle in place of those in this section.

12. Data Center Environment and Physical Security. The following is a general description of Oracle's various data center environments and efforts to ensure physical security in these environments.

    a. Physical Security Staffing. Each Oracle data center is staffed by onsite security personnel and monitored by a security organization responsible for continuous physical security functions.

    b. Physical Security Access Procedures. Formal access procedures exist for allowing physical access to the data centers.

    c. Physical Security Devices. Data centers employ electronic access control systems that are linked to a system alarm. Unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate.

    d. Redundancy. Oracle data centers are designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate single points of failure. In addition, Oracle has in place a procedure for recovering Customer Data and restoring service to a secondary data center in the event the Primary DC is declared by Oracle to be inoperable due to a catastrophic disaster.

    e. Power. The data center electrical power systems are designed to be fully redundant and maintainable without interruption to continuous operations. Backup power is provided by various mechanisms including the use of batteries and generators. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, overvoltage, undervoltage, and out-of-tolerance frequency conditions.

13. Risk Assessments. Oracle shall perform a risk assessment of the OpenAir Service every year. This assessment shall include an evaluation of risks to the confidentiality, integrity, and availability of Customer Data which resides on the OpenAir Service and a documented plan to correct or mitigate those risks in its security policies.

14. Use of Services. The OpenAir Service may not be delivered to or accessed by Users in Venezuela, nor may the OpenAir Service or any output from the Services be used for the benefit of any individuals or entities in Venezuela including, without limitation, the Government of Venezuela.

15. Definitions.

"**Primary DC**" shall mean the primary data center in which Customer Data is stored.

"**Safeguards**" shall mean physical and technical safeguards.

"**Security Incidents**" shall mean an actual unauthorized disclosure, or reasonable belief that there has been an unauthorized disclosure, by Oracle of Customer Data containing unencrypted personally identifiable information to any unauthorized person or entity.

[1]For clarity, the Safeguards set forth in this Addendum do not apply to any Third-Party Applications and may not apply to optional services subsequently ordered or activated by Customer that are subject to different terms.