OpenAir Services Data Security Addendum

OpenAir shall maintain commercially reasonable administrative, Safeguards designed for the protection, confidentiality and integrity of Customer Data. As of the Effective Date, such Safeguards are described below in this Data Security Addendum; provided, however, that Customer acknowledges and agrees that such Safeguards described in this Data Security Addendum are not comprehensive and such Safeguards may change during the Term of the Agreement, as applicable third party security audits, compliance standards and/or certifications evolve/change over time. For the Term of this Agreement, OpenAir shall comply with all obligations regarding Customer Data under the Agreement, including without limitation OpenAir's obligations to maintain commercially reasonable Safeguards as provided herein.

1. Security Policy. Oracle NetSuite 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 OpenAir security.

2. OpenAir Security Organization. Oracle NetSuite has, and will continue to have, a dedicated security organization that is responsible for the ongoing monitoring of OpenAir's security infrastructure, the review of OpenAir 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. OpenAir 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 will be destroyed in accordance with NIST 800-88 (or similar data destruction standard) at the Moderate level of sensitivity.

4. Data Transmission. OpenAir will use strong cryptography and security protocols consistent with industry standards, as documented in the User Guides for the Service.

5. Change Management. OpenAir 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. OpenAir servers will use a hardened operating system implementation customized for the Service. OpenAir will maintain a risk-based prioritized patch management policy.

7. Access Control and Privilege Management. OpenAir 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 OpenAir 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 in the Service.

10. Network Connectivity Security Requirements. OpenAir will protect its infrastructure with multiple levels of secure network devices.

11. Data Center Environment and Physical Security. The following is a general description of OpenAir's various data center environments and efforts to ensure physical security in these environments.
    a. Physical Security Staffing. Each OpenAir data center includes security personnel onsite and a security organization who are responsible for physical security functions 24 hours a day, 7 days a week.
    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. OpenAir 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, OpenAir has in place a procedure for recovering Customer Data and Service to a secondary data center in the event the Primary DC is declared by OpenAir 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 impact to continuous operations, 24 hours a day, and 7 days a week. Backup power is provided by various mechanisms including, but not limited to UPS batteries. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. Diesel engine generators are in place to provide power to critical equipment and customer loads.

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

13. 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 OpenAir of Customer Data containing unencrypted personally identifiable information to any unauthorized person or entity.