NETSUITE CONNECTORS DATA SECURITY ADDENDUM

For the NetSuite Connectors Service Cloud Service procured on the applicable Order, Oracle shall maintain commercially reasonable administrative Safeguards designed for the protection, confidentiality and integrity of Subscriber Data. All such safeguards shall be commensurate with the importance of the Subscriber 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 Order, such Safeguards are described below in this Addendum[1]; provided, however, that Subscriber acknowledges and agrees that such Safeguards described in this Addendum are not comprehensive and such Safeguards may change during the term of the applicable Order, 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 NetSuite Connectors Service Cloud Services during the term of the applicable Order. For the Term of the Agreement, Oracle shall comply with all obligations regarding Subscriber Data under the applicable Order, 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 and privacy training for Oracle security personnel supporting the NetSuite Connectors Cloud Service.

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 Subscriber Data will be secured and hardened in accordance with industry standard practices, such as:

   a. 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.

   b. Decommissioned media containing Subscriber Data will be destroyed in accordance with NIST 800-88 Revision 2 (or similar data destruction standard).

   c. Subscriber Data will be logically segmented from Oracle and other Oracle subscribers' data.

4. Data Transmission. Oracle will use strong cryptography and security protocols consistent with industry standards.

5. Incident Response. Oracle will monitor a variety of communication channels for known incidents, and Oracle's security team will react promptly to such known incidents. In the event of a Security Incident, Oracle will: (i) notify Subscriber in accordance with Oracle's obligations under applicable law or regulatory requirement, to the extent an applicable security breach law applies to such Security Incident; and (ii) perform a penetration test after corrective actions are implemented, if applicable, with a test results summary to be provided to Subscriber, such test results to be deemed Oracle Confidential Information.

6. 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.

7. Server Operating Systems. Oracle servers will use a hardened operating system implementation for the NetSuite Connectors Service. Oracle will maintain a risk-based prioritized patch management policy.

8. 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.

9. User Accounts. Subscriber will have control over the creation, deletion, and suspension of User roles within the Service.

10. Oracle Responsibilities and Policy Controls. Oracle will implement measures to ensure Subscriber Data is processed only in accordance with the instructions provided by the Subscriber.

11. Password Policy. Oracle provides a strong password policy to subscribers when they create or reset their password.

[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 Subscriber that are subject to different terms.

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

14. Data Center Environment and Physical Security. Oracle reviews available data center provider audit reports (e.g., SOC 1 and SOC 2) to ensure the following controls are in place:

a. Physical Security Staffing. Each 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. 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 uninterruptible and consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions.

e. Redundancy. The 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. Oracle has in place a procedure for recovering Subscriber Data and Service to a secondary data center in the event the Primary DC is declared by Oracle to be inoperable due to a catastrophic disaster. Oracle implements measures to ensure Subscriber Data is protected from accidental destruction or loss.

15. Risk Assessments. Oracle shall perform a risk assessment of the NetSuite Connectors Service every year. This assessment shall include an evaluation of risks to the confidentiality, integrity, and availability of Subscriber Data which resides on the NetSuite Connectors Service and a documented plan to correct or mitigate identified risks to an acceptable residual-risk level.

16. Handling of Personal Data. Oracle will process Personal Data as part of the provision of its services in accordance with its services agreement with the Subscriber and will be responsible for the compliance of its respective obligations under the applicable data protection laws. In handling and processing of Personal Data, Oracle shall implement and maintain appropriate technical and organizational security measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

17. Use of Services. The NetSuite Connectors Cloud Service may not be delivered to or accessed by Users in Venezuela, nor may the NetSuite Connectors Cloud 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.

18. Definitions.

"**Primary DC**" shall mean the primary data center in which Subscriber 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 Subscriber Data containing unencrypted information to any unauthorized person or entity.

"**Personal Data**" shall have the same meaning as the term "personal information", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.