Oracle Consulting & Advanced Customer Services Security Practices

Effective Date: 15 May 2018

Introduction & Scope

This document describes the security practices that Oracle organizations performing consulting services, and Oracle's Advanced Customer Services ("ACS") organization (for purposes of this document all such organizations collectively "Oracle") follow when performing such consulting or ACS services ("services") under the terms of your master agreement and applicable order for services (collectively the "order"). It also clarifies your security obligations with respect to your environments and the data therein. These practices supplement the Oracle Corporate Security Practices, which are incorporated herein by reference. 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 your order.

I. Definitions

The term "environment(s)" means your technology environments to which you grant Oracle access in order to provide the services under the order. The term "subcontractors" means subcontractors retained by Oracle and its subsidiaries that assist in performing the services.

II. Security Policies

Oracle's Corporate Security Practices cover the management of security for both its internal operations as well as the services Oracle provides to its customers, and apply to all Oracle employees. These policies, which are generally aligned with the ISO 27002 Code of Practice and ISO 27001 standards, govern all areas of security applicable to the services. You are strongly encouraged to implement your own comprehensive system of policies, standards and procedures, according to your risk-based assessments and business requirements.

III. Network Security

Oracle takes the following steps to secure access to the environments:

- Oracle employs Intrusion Detection Systems (IDS) within the Oracle network to intercept and respond to security events as they are identified. Oracle utilizes a network-based monitoring approach designed to detect attacks on open firewalls ports within Oracle's network. IDS events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT or Security department for review and response to potential threats.

- Oracle uses router rules, access control lists and segmentation on the Oracle network.

- Oracle's IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication; usage is audited.

- When Oracle accesses the environments residing on your system over the Internet, it uses only (a) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (b) technology permitted by your network administrator (e.g., direct dial-up or DSL if permitted on your network). Unless otherwise specified in the order, in (a) above, Oracle uses Oracle Continuous Connection Network (OCCN), which utilizes a persistent VPN tunnel and software VPN Combination, for Internet-based connections to the environments.

- Oracle may also use a desktop/laptop client based product when it accesses the environments residing on your system over the Internet. Examples include: Cisco Software VPN, Nortel Software VPN, Checkpoint Software VPN, Netscreen Software VPN, Point-To-Point Tunneling Protocol (PPTP), Neoteris Secure Sockets Layer (SSL) VPN, Aventail SSL VPN.

IV. Data Management/Protection

Oracle generally does not require or request access to production data in order to provide services. You are responsible for providing Oracle access to production data in a development or test environment and/or to a production computing environment only to the extent necessary to perform the services. The following applies to the extent that you have provided production data necessary to perform the services to Oracle.

Data Management: During the performance of the services, you maintain control over and responsibility for any production data residing in the environments. Oracle does not and will not:

- Change any production data, other than as required for the performance of the services.
- Have any role in determining or maintaining the accuracy of any production data.
- Control how production data is hosted, processed, stored or destroyed by you.
- Control your access to production data, other than restricting access to production data through applying physical and logical access controls, as applicable, as part of the services.

Deletion of Production Data: Upon termination of the services or at your request, Oracle will delete your production 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. Unless otherwise specified in writing, Oracle will archive production data on tape for six months following termination of the services.

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 may send

Oracle's Global Information Security organization a written request, including a detailed audit plan, at least six 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 your order.

V. Access Control

Account Provisioning and Passwords: Oracle requires the following standards for provisioning access to and creating passwords for the environments that are in the control of Oracle:

- Access is provisioned on a need to know basis.
- Passwords must conform to the strong password guidelines that include complexity, expiration, and length. Passwords are not permitted to be written down or stored on-line unencrypted.
- Passwords are treated as Oracle confidential information.
- At your request, Oracle will agree with you on a schedule for periodic password changes for credentials you have provided to Oracle to your systems.
- User IDs and passwords to your systems are not communicated to any other person without your prior authorization.

General Access: 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.

VI. Additional Oracle Practices

Information Security Managers: Oracle Consulting and ACS have appointed an Information Security Manager (ISM) to coordinate with Oracle Global Information Security (GIS) by serving as a resource to help identify strategic and practical security issues within the organization. The ISM serves as an advocate within Oracle Consulting and ACS to communicate information security awareness to Oracle Consulting and ACS employees and management and work collectively with that group to help implement and comply with Oracle's corporate security practices, policies and initiatives.

VII. Your Obligations

- You are responsible for all aspects of the collection of data, including determining and controlling the scope and purpose of collection. If you provide any personally identifiable information to Oracle for use in the performance of the services, you are responsible for sending any required notices and/or obtaining any required consents necessary for Oracle to perform the services. Oracle does not and will not collect data from data subjects or communicate with data subjects about their data.

- You will limit Oracle's access to your data to the extent necessary for Oracle to perform the services. You will prevent Oracle from accessing any health, payment card or other sensitive data that requires protections greater than those identified herein unless the parties specify the security measures applicable to Oracle's treatment of such data in the applicable order for services.

- You are responsible for managing Oracle's access to your systems, including providing unique accounts and user IDs where necessary.