Appendix 3 – Source Code Protection and Secure Development

This Appendix 3 to the Oracle Supplier Information and Physical Security Standards applies to Suppliers that are provided access to Oracle source code for the purpose of development or co-development. This Appendix sets forth requirements that are applicable when a Supplier is accessing, developing, transferring or storing Oracle source code. These terms are in addition to the terms of the Oracle Supplier Information and Physical Security Standards (the Standards) and all definitions in the Standards apply. Additional requirements may be included in any contract, agreement or statement of work.

Part A of this Appendix applies to all Suppliers that access, create, maintain, modify and/or use the Oracle source code for the purposes defined in the agreement. **To the extent a Supplier stores Oracle source code, Part B of this Appendix shall also apply.**

The following definitions apply to this Appendix:

“source code” means anything written in a computer programming language, including software that is executed on a computer and firmware that is executed within a dedicated hardware component; source code does not include design materials, documentation or compiled objects.

“source code repository” means a revision control system for source code, in order to control the access, creation, maintenance, modification and use of source code.

Part A

1. Security policies and practices

Supplier must document, maintain and apply the following organizational policies and practices:

1.1 A source code protection policy that states how source code must be handled and protected across the organization.

1.2 Documented secure coding practices that set forth secure coding and secure by design principles that all developers are required to apply when creating source code.

1.3 A secure development methodology that is integrated in to the Software Development Life Cycle (“SDLC”) and that (a) encompasses security principles throughout development and testing, and (b) addresses vulnerability management throughout the software lifecycle.

2. Secure Development Training

2.1 Supplier must provide secure coding training for all personnel that are involved in the development of Oracle source code. The training should be provided by, or at minimum aligned with, a recognized industry body such as Open Web Application Security Project (“OWASP”). The training must encompass secure coding principles and how to apply them throughout the software development process.

3. Software Development Life Cycle

In order to ensure security controls are implemented throughout the development processes, Supplier must ensure the following:

3.1 Only authorized personnel may access Oracle source code and only from Supplier-managed devices that meet the security requirements specified in the Standards and from locations set forth in the agreement.

3.2 Authorized personnel must not transfer or share Oracle source code with other Supplier employees or individuals who are not authorized to access or handle Oracle source code and are not involved in the delivery of Supplier’s services to Oracle.

3.3 Supplier must only use encrypted transport protocols (e.g., SFTP, SCP) when transferring, downloading, uploading or otherwise accessing Oracle source code.

3.4 Supplier must never store or share Oracle source code using non-Oracle approved public/cloud storage/collaboration services.

3.5 Supplier is responsible for ensuring that all Oracle source code is stored in a source code repository. Oracle source code must only be accessed and stored on computers located on Supplier's premises (laptops/desktops) while authorized personnel are actively working on the code. Oracle source code must be transferred and stored in a source code repository at all other times.

3.6 Oracle source code must not be stored on or accessed from any type of portable device (e.g., smartphone, tablet) unless required for the specific purpose of developing and testing mobile code/applications.

3.7 Supplier may only store Oracle source code for as long as it is required and for the purpose set forth in the agreement. Supplier must securely delete Oracle source code from all computers and devices, when the services are completed or terminated, unless Oracle has approved in writing that Oracle source code can be retained for an agreed period of time. After the retention period has expired, all Oracle source code in Supplier's possession or control must be permanently deleted from all computers, devices and backup media. Supplier must promptly provide to Oracle written confirmation of deletion of Oracle source code.

3.8 Supplier shall keep an accurate and up-to-date inventory for all Oracle source code in Supplier's possession. Such inventory should include a detailed description of the physical device name, device type, device location and purpose (e.g., source code repository, test system, build system) and the names of the system owners.

Part B

4. Source Code Repository systems

All source code repositories used to store Oracle source code must meet the following requirements:

4.1 The manager responsible for the Supplier's services to Oracle must approve individual access to a source code repository containing Oracle source code in advance. Supplier must ensure that approval is only given to authorized personnel directly involved in the provision of services to Oracle, as specified in the agreement. Supplier must further restrict access based upon specific roles (e.g., build engineers, release engineers) such that authorized personnel are only given access to Oracle source code files required to complete the individual's tasks.

4.2 Supplier must perform monthly account audits to ensure Oracle source code access remains restricted to authorized personnel only. Supplier must report as quickly as possible to Oracle any event that creates reasonable suspicion of unauthorized access to Oracle source code, as outlined in "Part F: Security Incident Management and Reporting" section of the Standards.

4.3 Supplier's repositories must retain records of Oracle source code changes. Such records must associate code changes with the individual who committed the change and the date and time of the change in Universal Coordinated Time (UTC). The records must allow individual changes to part of an object under source code control (such as a single line of code) to be traced back to the individual who committed it to the source code repository.

4.4 Individual user accounts must be associated with a single individual, and shared or generic accounts must not be used. Individual user accounts must be promptly disabled if the individual: (i) is terminated or otherwise ceases to work for Supplier, (ii) is no longer involved in providing the services to Oracle, (iii) completes assigned tasks or otherwise no longer requires access to Oracle source code.

4.5 Supplier must retain Source code repository access and activity records/logs for as long as specified in the agreement, but otherwise no less than six (6) months following the completion or termination of the services. Supplier records must be available for inspection by Oracle upon written request.

4.6 The operating system and applications installed on the source code repository must be installed, configured and maintained by Supplier in a secure manner. Supplier must implement system and log monitoring to prevent unauthorized modification of repository content and to monitor access. All changes to the operating system and applications must be controlled by the use of formal change control procedures.

4.7 Supplier must perform regular incremental backups and full backups of source code repositories. If a remote backup service is used, Oracle source code must be encrypted during transfer. All backups must be encrypted when stored on backup systems or media.

Effective Date: February 18, 2016