Appendix 2 – Supplier Data Center / Co-Location Security Standard

This document applies to Suppliers who provide data center/co-location services (including, without limitation, space, racks, power and cooling) to Oracle for its internal use or for the provision of Oracle services to its customers. 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.

1. Supplier Data Center Security Operations and Oversight

The Supplier will:

1.1 Maintain SSAE 16 and/or ISAE 3402 SOC 2 reports (covering at least "Security", "Confidentiality" and "Availability") with audit and reporting periods no greater than 12 months that are current for the entire duration of the services. Supplier will provide complete, unqualified reports of such assessments to Oracle upon request.

1.2 Maintain policies, standards and procedures that are consistent with ISO 27001 and have a scope that encompass the facilities, networks, computers and processes used to perform the services.

1.3 Maintain any geographic specific security standards and certifications applicable to the Supplier's performance of the contracted services for Oracle.

1.4 Maintain controls specified in Oracle's agreement with Supplier that enable Oracle to meet its compliance requirements to store/process specific types of regulated data, e.g. Payment Card Industry Payment Card Data (PCI), HIPAA/HITECH Protected Health Information (PHI).

1.5 Utilize security-focused Standard Operating Procedures (SOPs) to deliver the services. The SOPs must describe the detailed activities and tasks, as well as provide direction, to be undertaken by Supplier data center personnel when delivering services to Oracle.

1.6 Continually evaluate its exposure to security and other threats and take appropriate measures to address the associated risks to facilities, computers, environments, and Oracle confidential information.

2. Security Audit and Assessment

The objectives of security assessments are to evaluate whether all aspects of the services are designed and delivered in compliance with the requirements in the Standards and this Appendix 2 and to ensure no material vulnerabilities exist within the Supplier's facilities.

2.1 Upon reasonable notice, Supplier will permit Oracle and/or Oracle customers (including government regulators requiring inspections of Oracle or its customers) whose data is stored, accessed or otherwise processed in the Supplier's data center, to perform security assessments.

2.2 Security assessments may include the following areas for review, as applicable to the services:

a. Physical, administrative, operational and technical controls for the data center facility and all associated operations.

b. Procedures to evaluate Supplier's incident management process and response to external/internal threats and incidents.

c. Network and system vulnerability assessments.

2.3 Supplier will act promptly to resolve assessment findings and implement recommendations made to address shortcomings identified for specific activities and/or operational areas. Resolution for the most critical findings must be monitored and regular progress reported to Oracle until they are fully implemented.

3. Physical Security

The following minimum physical security requirements apply to all Supplier co-location/external data center supplier facilities. Additional physical security measures may be agreed to by the parties in the Agreement to the extent required due to contractual obligations with Oracle's customers or based on a physical security risk assessment.

3.1 The facility must be equipped with an electronic centrally managed access control system and perimeter door alarms. All doors giving access to the segregated area housing any Oracle assets or environments must have an electronic dual identification method, such as a PIN pad or biometrics. There must also be an anti-pass back capability.

3.2 The access control system must record and store entry and exit details for all employees and visitors for at least 90 days. Access privileges must be removed immediately upon termination of an employee, including revocation of access to facilities and application account removal. The database must be reviewed every 6 months. Authorized access lists and reports must be provided to Oracle upon request.

3.3 A CCTV system with coverage sufficient to capture images of all Oracle assets and access/egress points, including emergency exits, and area lighting sufficient to support the CCTV system during hours of darkness, must be in place and record activity 24hours/7days. Images must be retained for a minimum of 90 days unless otherwise prescribed by local law. Oracle must be given access to the CCTV images upon request. All recording equipment and tapes will be stored in a secure room to which access is restricted to authorised personnel only.

3.4 The facility must have dedicated 24 hour on-site guarding. Routine check calls must be maintained between the on-duty officers and their central control. A means of communicating duress must also be utilized.

3.5 In addition to the real-time alarm monitoring provided by the on-site security force, real-time alarm monitoring by an alarm company or a law enforcement agency central station must also be provided. All alarms must be responded to immediately.

3.6 All windows must be alarmed or hardened so they are capable of providing a minimum 20-minute defence period.

3.7 Perimeter alarms must trigger a loud local noise. Door forced alarms must be immediate. Door held alarms must be set to a default of 30 seconds.

3.8 If recommended by an Oracle Global Physical Security risk assessment, the facility must be enclosed with fencing and gating that enables access to be controlled and limited to authorised personnel.

3.9 Employees must be provided with training that informs them of their individual responsibilities and the actions to take in the event of an incident, such as, how to report suspicious activity or the immediate actions to be taken in the event of robbery or facility takeover.

3.10 The contracting Oracle line of business must be given immediate notification if any loss or damage of Oracle assets is suspected or occurs; when theft is suspected, Oracle Global Physical Security must also be notified immediately.

3.11 A badging process that identifies employees and visitors must be employed. All visitors must be escorted.

Supporting Infrastructure

3.12 All infrastructure must be sited or protected to reduce the risks from environmental threats and hazards.

3.13 Supporting infrastructure located inside a facility, such as network infrastructure, demarcation points, communications and any other infrastructure used to provide services to Oracle, must have physical security protections designed to ensure access to those areas is limited to authorized personnel, monitored and controlled.

3.14 Supporting infrastructure located outside the facility, such as generators, cooling towers, fuel tanks, data and communication lines, must have physical security protections designed to ensure access to those areas is limited to authorized personnel, monitored and controlled.

3.15 The facility must have centrally managed and regularly maintained temperature and humidity controls, heat and smoke detection, and fire suppression systems in place. Maintenance reports must be provided to Oracle on request

3.16 Backup power must be available to support the security alarm, access control, CCTV systems, environmental controls, and other supporting security infrastructure. Where batteries are used as the backup power source, a minimum of 8 hours of power must be available.

Oracle Environment

3.17 Supporting infrastructure and systems within the Co-location/External Center Data facility used to provide services to Oracle must be located in a distinct and segregated area from other hosted systems. Segregation must be by physical barriers, such as solid walls or metal security caged area. Segregation must continue below floor and above the ceiling if the floor/ceiling height or type allows the physical barrier to be bypassed.

3.18 The facility must not identify or mark Oracle assets or dedicated areas in a manner that makes them visible to public or general access areas, such as by placing “Oracle” on Door signs that can be seen from the public lobby or a space accessed by other customers.

3.19 The supplier must limit its employees and agents access to assets, computers, confidential information and environments to that which is specifically necessary to perform services for Oracle under the specified agreement or statement of work.

3.20 Oracle will provide Supplier with a list of approved Oracle employees and vendors that are permitted to have access to the Oracle assets, computers and environments. All authorized visitors must present a photo ID card issued by their employers and/or a passport, driving license or other Government issued photo identification. All visits must be prearranged and logged.

3.21 Photography of the area containing Oracle assets and environment is prohibited, unless authorized in writing by Oracle.

3.22 Photography of physical security measures, such as CCTV cameras, access control systems and alarm panels, is not permitted under any circumstances.

Effective Date: December 1, 2013