ORACLE SUPPLIER INFORMATION & PHYSICAL SECURITY STANDARDS

These Supplier Information and Physical Security Standards (the "Standards") list the security controls that Oracle's Suppliers are required to adopt when (a) accessing Oracle or Oracle customer facilities, networks and/or information systems, (b) handling Oracle confidential information or (c) having custody of Oracle hardware assets.

Supplier is responsible for compliance with these Standards by its personnel, including ensuring that all personnel are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier's agreement or individual statement of work.

Part A: Definitions

Part B: Personnel/Human Resources Security

Part C: Business Continuity and Disaster Recovery

Part D: Information Security Organization and Policy

Part E: Compliance and Audit

Part F: Security Incident Management and Reporting

Part G: IT Security Standards

Part H: Physical and Environmental Security

Appendix 1: Supply Chain Physical Security Standard

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

Appendix 3: Source Code Protection and Secure Development Standard

Appendix 1, Supply Chain Physical Security Standard, applies only if (a) the facilities of Suppliers in Oracle's hardware supply chain are used for manufacturing, assembly, storage, stocking, handling, distribution, transportation, delivery, support, repair, re-manufacture, recycling, scrap, and disposal of Oracle products or assets, or (b) Suppliers have physical custody of Oracle products or assets and are notified in their contracts or subsequently in writing that they must comply with Appendix 1.

Appendix 2, Supplier Data Center / Co-Location Security Standard, applies only to Suppliers who provide data center/co-location services (including space, racks, power and cooling) to Oracle for its internal use or for the provision of services to its customers.

Appendix 3, Source Code Protection and Secure Development Standard applies only to Suppliers that are provided with or have access to Oracle source code for the purpose of development or co-development.

Part A: Definitions

The following definitions apply to these Standards:

"**agreement**" means an agreement between Oracle and a Supplier under which (a) Supplier performs services for Oracle and/or (b) Supplier is provided access to Oracle facilities, network(s), information systems and/or confidential information.

"applications" means middleware, databases, applications, web portals or other software that are used in the delivery of services to Oracle.

"asset" means any tangible Oracle owned item for which a Supplier has responsibility.

“**computer**” means any desktop or laptop computer, mobile device (e.g., cellular phone, Smartphone, tablet), server and/or storage device that (i) is involved in the performance of the services, (ii) may be used to access a network or an environment, or (iii) may access or store confidential information.

“**information systems**” means any system, including but not limited to development, test, stage and production systems, or storage/backup systems, that (a) are involved in the performance of the services, (b) may access, process or store Oracle confidential information.

“**confidential information**” means all Oracle confidential information to which Supplier may be provided access in connection with the performance of services , including without limitation personal information (PI); intellectual property (IP); source code; passwords; information concerning Oracle’s customers, suppliers or partners; any data stored in or provided from the information systems of Oracle or its customers, suppliers or partners; and any other Oracle confidential information as defined in an agreement. References in this document to “confidential information” shall be deemed to include confidential information of Oracle customers, suppliers or partners to which Supplier is provided access in connection with providing services.

“electronic media” means hard disk, solid state disk, DVD/CD, tape or any other form of media that can store electronic information.

“facilities” means (a) any offices, data centers and all other locations (whether owned or managed by Oracle, an Oracle customer, Supplier or a third-party) from which Oracle confidential information, information systems or networks may be accessed or (b) any permanent or non permanent location handling or storing Oracle assets. References in this document to (i) “Oracle facilities” shall be deemed to include facilities of Oracle customers, and (ii) “Supplier facilities” shall be deemed to include third-party facilities used by Supplier.

“**network**” means any Oracle networks to which Supplier is provided access in connection with the performance of services under an agreement and/or any Supplier networks that are used to access confidential information or information systems.

“**network devices**” means routers, switches, load balancers, firewalls and virtual private network (VPN) devices.

“personnel” means all Supplier employees, contractors, sub-contractors and agents who are provided access to facilities, networks, information systems and/or confidential information.

“**PI**” or “**personal information**” means any information to which Supplier is provided access that could identify any individual, either directly or indirectly, including without limitation the individual’s name; address; government identification/national identification number; health, financial or employment information, phone number, e-mail address, IP address.

“product” means a hardware or software component or assembled good manufactured for or supplied to Oracle.

“security incident” means (a) unauthorized access to confidential information or information systems, (b) misappropriation or alteration of any or confidential information, or (c) theft, loss or damage to assets.

“**services**” means the work to be performed by Supplier for Oracle as specified in an agreement, contract, or statement of work.

“**Supplier**” means an entity (including its personnel) that (a) performs services under an agreement and/or (b) is granted access to Oracle facilities, networks, information systems and/or confidential information.

“**Supplier facilities**” means all facilities used by Supplier, including third-party facilities.

Part B: Personnel/Human Resources (HR) security

B.1 Supplier will perform background checks, consistent with local laws and regulations, for all personnel. The level of verification performed should be proportional to risk correlated to roles within the organization.

B.2 Supplier personnel are required to agree, in writing, to abide by Supplier's security requirements and organizational policies.

B.3 Supplier must have a comprehensive security awareness program for all personnel that encompasses education, training and updates for security policies, procedures and requirements. Training must be provided at time of hiring and repeated at regular intervals thereafter (no less than every two years).

B.4 Supplier must have formal disciplinary processes in place for personnel and will take appropriate action against personnel who violate Supplier's organizational policies, based upon the nature and gravity of the violation.

B.5 Upon termination of personnel employment, Supplier will promptly remove access to information systems, networks and applications and confirm personnel have not retained any confidential information.

B.6 Supplier is authorized to use subcontractors for the provision of the Services as long as they are contractually bound to comply with nondisclosure terms and security standards consistent with those set forth in the agreement and this document. Supplier will maintain a list specifying its subcontractors, the country of destination of the data, and will provide that list to Oracle upon reasonable notice. Oracle may, reject the use of any subcontractor for justified reasons.

Part C: Business Continuity and Disaster Recovery

C.1 Suppliers must have a Disaster Recovery (DR) program and maintain a documented organizational Business Continuity Plan (BCP). The program and plans must be designed to ensure that Supplier can continue to function through operational interruption and continue to provide services, as specified in its agreement with Oracle.

C.2 Supplier must ensure that the scope of the BCP covers all locations, personnel and information systems that are used to perform services for Oracle.

C.3 The BCP must be tested on a regular basis (at minimum, on an annual basis). Supplier will document the results and provide documentation for Oracle's review to confirm that the tests were performed.

C.4 Supplier must promptly notify Oracle in the event the DR plan is executed and report the potential impact on Supplier's capability to perform services for Oracle.

Part D: Information Security Organization, Policy and Procedures

D.1 Supplier must have clearly defined organizational information security roles, responsibilities and accountability.

D.2 Supplier must publish and maintain formal written information security policies. Information security policies must be approved by management and communicate personnel's obligations to protect confidential information and the acceptable use and protection of all information assets.

D.3 Supplier must classify and label Information in accordance with their information classification scheme and in terms of its sensitivity.

D.4 Supplier will implement security processes for managing suppliers throughout the business relationship lifecycle.

D.5 Supplier will maintain an inventory of assets that includes all business critical information systems and information processing sites that are used in the delivery of services to Oracle. The asset inventory should be accurate, up to date and have owners assigned to each asset.

D.6 Supplier will maintain a complete list of all personnel with permission to access Oracle facilities, information systems, networks and applications, including their geographic location.

Part E: Compliance and Assessments

E.1 Regulatory Compliance

E.1.1 If services involve Payment Card Information (PCI), Supplier will maintain compliance with the current version of the Data Security Standards (DSS) from the Payment Card Industry Security Standards Council (PCI SSC) for the duration of the services provided to Oracle. On request, Supplier will provide Oracle with the most recent PCI SSC "Attestation of Compliance" (AoC) reports prepared by a third party PCI Qualified Security Assessor (QSA) for both Supplier's systems and for any third-parties used by the Supplier for handling payment card data.

E.1.2 Supplier will inform Oracle if Supplier has reason to believe that legislation applicable to the Supplier prevent it from fulfilling the obligations relating to treatment of Oracle personal information.

E.2 Security Compliance

E.2.1 If Supplier is provided access to personal information by Oracle, or is otherwise processed by Supplier on Oracle's behalf, Supplier must sign the Oracle Supplier Data Processing Agreement (SDPA).

E.2.2 All Suppliers accessing Oracle's network must execute an Oracle Network Access Agreement (NAA) and have a valid Project Exhibit (PE).

E.2.3 If requested, Supplier will confirm to Oracle in writing its compliance with the requirements of these Standards and will provide written responses to any questions that Oracle submits to Supplier about its security practices. Supplier will provide Oracle with the contact information of the person(s) Oracle may contact in relation to any information security related issues.

E.3 Security Assessments

E.3.1 Oracle may perform security assessments upon reasonable notice to confirm compliance with these Standards. Supplier will also ensure that Oracle has direct access to assess subcontractors, upon reasonable notice, in order to confirm compliance with these standards.

E.3.2 Supplier must promptly correct any noncompliance issues identified during the security assessment.

Part F: Security Incident Management and Reporting

F.1 Supplier must have documented information security incident procedures that enable effective and orderly management of security incidents. The procedures must cover the reporting, analysis, monitoring and resolution of security incidents.

F.2 Reported security incidents should be verified and then analysed to determine their impact. All confirmed incidents should be classified, prioritized and documented.

F.3 Security incidents should be handled by a dedicated security incident response team or personnel who are trained in handling and assessing security incidents in order to ensure appropriate procedures are followed for the identification, collection, acquisition and preservation of information.

F.4 Supplier must promptly report any observed or suspected information security incidents relating to the Oracle services, to their business contacts at Oracle, for the applicable services impacted by the security incident. Confirmed security incidents must be reported to security_breach_ww@oracle.com

F.5 Other than to law enforcement or as otherwise required by law, Supplier may not make or permit any statements concerning security incidents involving Oracle confidential information, information systems or assets to a third-party without the written authorization of Oracle's Legal Department, unless the statements do not identify or could not reasonably be used to identify Oracle as being impacted by the incident.

F.6 Unless prohibited by law, Supplier will promptly notify Oracle in the event it receives a request to provide access to Oracle confidential information or information systems.

G. IT Security Standards

G.1 IT Security Controls

G.1.1 Suppliers Information systems, network devices and applications should be configured and deployed using a secure baseline (hardened) and ports/services that are not used should be disabled.

G.1.2 Supplier must implement controls to restrict the connection times of idle/Inactive sessions on information systems, applications and network devices and terminate inactive sessions.

G.1.3 System clocks should be synchronized to a trusted time server source so that time/time zone is accurately maintained on all Information systems and network devices, to ensure logs files have consistent time stamp information recorded.

G.1.4 Supplier should have a defined security review processes for the deployment of new services that store/process Oracle confidential information.

G.1.5 Supplier will perform security assessments, scans and testing of information systems, networks and applications at planned intervals to verify compliance with organizational security policies and standards.

G.1.6 Supplier will maintain documented change management procedures that provide a consistent approach for controlling and identifying configuration changes for information systems, applications and network devices.

G.2 Network Security

G.2.1 Supplier will implement network security infrastructure such as Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and other security controls that provide continuous monitoring, restrict unauthorized network traffic, detect and limit the impact of attacks.

G.2.2 Network traffic should be appropriately segregated with routing and access controls separating traffic on internal networks from public or other untrusted networks.

G.2.3 Remote access in to the Suppliers network must be approved and restricted to authorized personnel. Remote access must be controlled by secure access control protocols, encryption and authentication.

G.2.4 If VPN access (either site-to-site or IPsec) is used to access Oracle networks and information systems, Supplier should segregate computers that remotely connect to Oracle (using either physical segregation or VLAN subnets) to prevent Oracle confidential information, networks and information systems from potentially being accessible or visible by other personnel on the Supplier's network.

G.2.5 To the extent permitted by law, Oracle reserves the right to monitor Supplier access to and use of Oracle information systems, networks and applications.

G.3 Logging

G.3.1 Supplier must maintain logs from information systems, network devices and applications for a minimum period of 90 days. Logs should be sufficiently detailed in order to assist in the identification of the source of an issue and enable a sequence of events to be recreated.

G.3.2 Logs must record date, time and source location (IP address/hostname) for all access attempts.

G.3.3 Logs must capture system and network security event information, alerts, failures, events and errors.

G.3.4 Integrity of logs files must be maintained and protected from tampering by restricting access to systems that store log information. Log files should be stored on a centralized log server.

G.4 Technical vulnerability and patch management

G.4.1 Supplier must track information from vendors and other sources in relation to technical vulnerabilities of operating systems, applications, and network devices; and must promptly evaluate exposure to reported vulnerabilities to ensure that appropriate measures are taken to address potential risks.

G.4.2 Supplier must have procedures for patch management processes that promptly apply patches for all operating systems, applications and network devices in a consistent, standardized and prioritized manner based on criticality and risk. If a security patch cannot be promptly applied due to requirements for testing, then effective risk mitigation controls must be implemented until such time patches can be applied.

G.4.3 Computers should be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.

G.4.4 Supplier must use anti-virus/malware detection software to prevent, detect and remove malicious code, e.g. malware, viruses, spyware and Trojans. The software must provide automated signature updates. The software should have functionality to detect if anti-virus/malware software on computers has been disabled or not receiving regular updates.

G.4.5 Automatic virus and malware scanning checks must be carried out on all e-mail attachments that are sent to or received from external sources. Attachments that are identified as containing malicious code must be removed and deleted.

G.5 Information Backup

G.5.1 Supplier must ensure that information systems, computers and software involved in the performance of the services provided to Oracle are backed up to online and/or offline storage. Backups must be tested in accordance with operational backup standards.

G.5.2 Backup media that leaves Supplier’s facility must be protected against unauthorized access, misuse or corruption during transportation. Oracle confidential data that is stored on backup media, if not already encrypted, must be encrypted using 128-bit or higher encryption.

G.6 Account Management

G.6.1 Supplier must have user account management procedures to support the secure creation, amendment and deletion of accounts on information systems, network devices and applications.

G.6.2 The procedures should include processes for ensuring that information systems, applications and network device owners authorize all new user account requests and identification of redundant accounts.

G.6.3 User accounts must be attributable to individuals (i.e. every account will have a unique login identifier and password). Supplier personnel should not share account credentials.

G.7 Access controls

G.7.1 Access controls must be implemented for information systems, networks and applications that verify the identity of all users and restrict access to authorized users.

G.7.2 Access controls must use a role based access model and differentiate access levels for end-users and privileged access (e.g. systems administrators).

G.7.3 Approvals for access requests must have appropriate segregation of duties, e.g. different personnel must perform the access authorization and access administration roles.

G.7.4 Access lists for information systems, network devices and applications must be reviewed on a regular basis and access removed when no longer required.

G.7.5 Access to Oracle information systems, networks and applications by Supplier personnel is limited to the purposes of performing services as specified in the agreement with Oracle.

G.8 Password Management

G.8.1 Strong password practices must be used that include minimum password length and require complexity (e.g. no dictionary words, use a mix of alpha numeric characters etc.).

G.8.2 Passwords must have a set expiration period that does not exceed six months.

G.8.3 Passwords must be distributed separately from account information, in a manner that ensures confidentially of information.

G.8.4 Passwords must be encrypted when transmitted between information systems, network devices and applications.

G.9 Protection of Oracle Confidential data

G.9.1 Supplier may access, use and process Oracle confidential information only on behalf of Oracle and only for the purposes specified in the agreement with Oracle and in compliance with these Standards.

G.9.2 Oracle confidential information stored on Suppliers computers and external electronic media (e.g. USB memory storage, tape) must be fully encrypted using 128-bit or higher encryption.

G.9.3 Oracle confidential information may not be stored on mobile devices or device media cards unless encrypted using 128-bit or higher encryption and devices are managed through centralized device management software that has the capability to remotely lock and wipe lost/stolen devices.

G.9.4 Supplier will delete Oracle confidential information upon Oracle's request, upon completion of services or upon the termination of services. Supplier may retain one copy of the foregoing materials, as required for regulatory retention purposes or by law, provided that any such copy is kept in encrypted format, is not used or accessed for any other purpose and is protected in accordance with the requirements of these Standards.

G.9.5 Electronic media containing Oracle confidential information must be sanitized before disposal using a process that assures data deletion and prevents data from being reconstructed or read, as prescribed in industry standards such as NIST SP 800-88 Revision 1 and DoD 5220.22-M. Defective electronic media containing Oracle confidential information should be physically destroyed

G.9.6 Oracle confidential information must not be transmitted using unencrypted (plain text) channels or services over public networks. Encrypted protocols that protect the transfer of information, for example, SSL, SFTP, TLS must be used.

G.9.7 Secure e-mail transport using Transport Layer Security (TLS) between Oracle mail gateways and Supplier mail gateways must be used to protect Oracle confidential information sent using e-mail.

G.9.8 Supplier will not permit the use of personal email accounts for exchanging Oracle confidential information.

G.9.9 Supplier should not use production systems that store or process Oracle confidential information for development, testing or staging purposes.

G.9.10 The use of public cloud storage services for the storage/exchange of Oracle confidential information must be agreed and approved by Oracle.

Part H: Basic Physical and Environmental Security

H.1. Supplier Facilities: Supplier must maintain the following controls at all Supplier facilities (including third party facilities used by Supplier) from which Oracle networks, information systems and/or confidential information may be accessed:

H.1.1 Supplier must maintain a physical security plan to protect offices and information processing facilities that addresses internal and external threats to sites. Plans must be reviewed and updated on at least an annual basis.

H.1.2 Sites must have secure entry points that restrict access and protect against unauthorized access. Access to all locations must be limited to authorized personnel and approved visitors. All visitors must be required to sign a visitor register. Entry points should have security cameras.

H.1.3 Reception areas for offices and information processing facilities should be manned by either a receptionist or security guard. Out of hours access should be monitored, recorded and controlled. Logs detailing access must be stored for a period of at least 90 days.

H.1.4 Supplier personnel and authorized visitors must be issued identification cards. Visitor identification cards must be distinguishable from Supplier personnel identification cards and must be retrieved and inventoried daily.

H.1.5 Access cards and keys that provide access to secure areas and information processing facilities such as data centres must be monitored and limited to authorized personnel. Regular reviews of access rights to must be performed.

H.1.6 Off-site removal of information systems, computers and network devices must be restricted, approved and authorized by asset owners and appropriate security departments.

H.1.7 A clear desk policy must be enforced in areas where Oracle confidential information is stored. Documents that contain Oracle confidential information must be secured when not in use.

H.2 Oracle Facilities: Supplier personnel must abide by the following requirements at Oracle facilities:

H.2.1 Supplier personnel are required to abide by Oracle's security requirements and direction when working at Oracle facilities. The security measures employed at Oracle facilities (e.g., use and placement of security cameras, use and placement of other physical and logical security controls) are Oracle confidential information. Personnel may not photograph or otherwise record Oracle facilities or infrastructure, unless required for the performance of services.

H.2.2 Supplier personnel may not access Oracle computers or networks unless access expressly authorized by Oracle personnel.

Effective Date: February 29, 2016