ORACLE

Oracle Supplier Information and Physical Security Standards

Effective Date: January 21, 2022

Contents

SCOPE

These Supplier Information and Physical Security Standards (the "Standards") list the minimum 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 OBLIGATIONS

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.

PART A: PERSONNEL/HUMAN RESOURCES SECURITY

A.1 Unless prescribed otherwise in the agreement, 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.

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

A.3 Supplier must have a comprehensive security awareness program for all personnel that encompasses education, training and updates for security policies, procedures and requirements. Security awareness training must occur at time of hiring and repeated at regular intervals thereafter (no less than every two (2) years).

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

A.5 Upon termination of employment, Supplier will promptly remove personnel access to information systems, networks, and applications. Personnel must also return all company provided computers, mobile devices and other equipment used to perform the services. Supplier will remind personnel that they must not retain any confidential information.

A.6 Unless otherwise specified in an Oracle Supplier Data Processing Agreement (SDPA), 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 these Standards.

A.7 Supplier will maintain a list of its authorized subcontractors, the country/countries to which confidential information may be transferred to or accessed from, a description of the services performed by such subcontractors, and make that list available to Oracle.

PART B: BUSINESS CONTINUITY AND DISASTER RECOVERY

B.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 the agreement.

B.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.

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

B.4 If there is an event, which will or does impact Supplier's capability to perform services for Oracle, including execution of the DR plan, Supplier must promptly notify their Oracle business contact.

Part C: Information Security Organization, Policies, and Procedures

C.1 Supplier must have clearly defined organizational IT/information security roles, responsibilities and accountability.

C.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 information.

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

C.4 Supplier will implement security processes for managing suppliers and subcontractors throughout the business relationship lifecycle.

C.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.

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

PART D: COMPLIANCE AND ASSESSMENTS

D.1 Regulatory Compliance

D.1.1 If services involve the processing of payment card information, 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.

D.2 Security Compliance and Assessments

D.2.1 If Supplier is provided access to Personal Information by Oracle or Oracle customers, or Personal Information is otherwise processed by Supplier on Oracle's or Oracle customer's behalf, Supplier must sign an Oracle SDPA.

D.2.2 All Suppliers accessing Oracle's network must execute an Oracle Network Access Agreement (NAA).

D.2.3 Supplier will provide Oracle with the contact information of the person(s) Oracle may contact in relation to any information security and/or compliance issues.

D.2.4 If requested, on an annual basis, Supplier will complete a documented security questionnaire and provide written responses about its security practices, to enable Oracle to assess compliance with the requirements of these Standards and applicable law.

D.2.5 If requested, in order to confirm compliance with these Standards, upon reasonable notice and in coordination with Supplier, Oracle may perform on-site security assessments.

D.2.6 Only when and to the extent required of Oracle by contract or applicable law, Supplier will ensure that Oracle has direct access to assess subcontractors.

D.2.7 Supplier must promptly correct any noncompliance issues identified during the documented and/or on-site security assessment process.

PART E: SECURITY INCIDENT MANAGEMENT AND REPORTING

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

E.2 Reported security incidents shall be verified and then analyzed to determine their impact. All confirmed incidents should be classified, prioritized and logged.

E.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.

E.4 Supplier must report security incidents of which they become aware relating to the Oracle services without undue delay (but at the latest within 24 hours) to their business contacts at Oracle for the applicable services impacted by the security incident and sending e-mail to security_breach_ww@oracle.com.

E.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.

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

PART F: IT SECURITY STANDARDS

F.1 IT Security Controls

F.1.1 Suppliers information systems, network devices, and applications should be configured and deployed using a secure baseline. Ports/services that are not used should be disabled.

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

F.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, network devices, and applications, to ensure logs files have consistent time stamp information recorded.

F.1.4 Prior to implementation of information systems, network devices, and applications that will be used to process/store Oracle confidential information, a security review process should be followed to validate security of the information sytems, network devices, and applications to identify and remediate critical security issues ahead of deployment.

F.1.5 Supplier will perform security assessments in the form of technical scans and testing of information systems, networks, and applications at planned intervals, at least annually, to verify compliance with organizational security policies and standards.

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

F.1.7 If mobile devices are used in the delivery of services to Oracle, devices should be managed using centralized solution that has the capability to remotely lock and wipe lost/stolen devices.

F.2 Network Security

F.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, have the capability to restrict unauthorized network traffic, detect and limit the impact of attacks.

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

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

F.2.4 Where applicable to services provided to Oracle, if VPN access (either site-to-site or IPsec) is used to connect to Oracle networks and information systems, Supplier must 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 network.

F.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.

F.3 Logging

F.3.1 Supplier must maintain logs from information systems, network devices, and applications for a minimum period of ninety (90) days and store log files on a centralized logging server. 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.

F.3.2 Logs must record when (date and time), who (such as user or service account) and where (IP address/hostname) for all access and authentication attempts.

F.3.3 Logs must capture information system, network device and application security related event information, alerts, failures, and errors.

F.3.4 Integrity of logs files must be maintained and protected from tampering by restricting access to systems that store log files.

F.3.5 Logs must be continually monitored, reviewed and analyzed for suspicious and unauthorized activity and to verify the integrity of the logging process.

F.4 Technical Vulnerability and Patch Management

F.4.1 Supplier must track information from technology vendors and other authoritative sources in relation to technical vulnerabilities of all technology in use, including hardware, operating systems, applications, and network devices; and must promptly evaluate exposure to reported vulnerabilities to ensure that appropriate measures are taken to address risk.

F.4.2 Supplier may only use technology vendors that provide patch updates. Supplier's own procedures must have patch and vulnerability management processes that promptly apply patches to all technology in use including hardware, operating systems, applications and network devices in a consistent, standardized and prioritized manner based upon criticality and risk. If a security patch cannot be promptly applied, then effective risk mitigation controls must be implemented until such time patches can be applied.

F.4.3 Laptop/desktop computers should be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.

F.4.4 Supplier must use endpoint protection, such as anti-virus/malware detection software. This software must be installed, configured, enabled, and updated to prevent, detect and remove malicious code, e.g. malware,

viruses, spyware and Trojans. Endpoint protection solutions should detect if the software has been removed, disabled, or is not receiving regular updates.

F.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.

F.5 Information Backup

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

F.5.2 Oracle confidential information that is stored in backups must be encrypted using AES-256-bit or higher encryption or other strong encryption standard depending on backup method. Where applicable, backups that leave Supplier's facility must be protected against unauthorized access, misuse or corruption during transportation and storage.

F.6 Account Management (inclusive of user, systems, and admin)

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

F.6.2 The procedures should include processes for ensuring that information systems, applications, and network device owners authorize all account requests and revoke any unnecessary access based on job role..

F.6.3 Supplier personnel must not share account credentials. All user accounts must be attributable to individuals (i.e. every account will have a unique authentication credential).

F.7 Access Controls

F.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.

F.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).

F.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.

F.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 such as personnel job role change or termination.

F.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.

F.8 Password Management

F.8.1 Account authentication credentials must be unique and not be reused for other accounts.

F.8.2 Password must have no less than a minimum of eight characters for password length and require character complexity (e.g. no dictionary words, use a mix of alpha numeric characters and symbols etc.). Multifactor authentication may be used in Supplier's discretion depending on Services.

F.8.3 Passwords must have a set expiration period that does not exceed six months.

F.8.4 Passwords must be distributed separately from account information.

F.8.5 Passwords must be encrypted when transmitted between information systems, network devices and applications.

F.9 Protection of Oracle Confidential Information

F.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 and in compliance with these Standards.

F.9.2 Where Oracle confidential information is stored on Supplier personnel laptop/desktop computers and external electronic media (e.g. USB drives), the media must be fully encrypted using AES-256-bit or higher encryption.

F.9.3 Oracle confidential information may not be stored on mobile devices unless the devices encrypts content stored on the device by default, or the devices and media cards are encrypted using AES-256-bit or higher encryption.

F.9.4 Supplier will delete Oracle confidential information upon Oracle's request, upon completion of services, or upon the termination of services. If required for regulatory retention purposes, by law, or as specified in the agreement, Supplier is permitted to retain one copy of the foregoing materials, as required, provided that any such copy is encrypted, is not used or accessed for any other purpose and is protected in accordance with the requirements of these Standards, and is promptly deletion if no longer required for regulatory retention purposes.

F.9.5 Electronic media that is decommissioned and has been used in the delivery of services to Oracle must be sanitized before disposal or repurposing, using a process that assures data deletion and prevents data from being reconstructed or read, as prescribed in a recognized standard (e.g. NIST SP 800-88). Defective electronic media containing Oracle confidential information must be physically destroyed

F.9.6 Oracle confidential information must be transmitted using encrypted protocols that protect the transfer of information, e.g., SFTP, TLS.

F.9.7 Where services require Oracle confidential information to be exchanged using e-mail, Transport Layer Security (TLS) between Oracle mail gateways and Supplier mail gateways must be used.

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

F.9.9 Supplier must not use Oracle confidential information from production systems for development, testing or staging purposes.

PART G: BASELINE PHYSICAL AND ENVIRONMENTAL SECURITY

G.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.

G.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.

G.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.

G.1.3 Access areas to information processing facilities should be manned by a 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.

G.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.

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

G.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.

G.1.7 Documents that contain Oracle confidential information must be kept in a secure location when not in use.

G.2 Oracle Facilities

Supplier personnel must abide by the following requirements at Oracle facilities.

G.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.

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

PART H: DEFINITIONS

The following definitions apply to these Standards:

"**agreement**" means, individually or collectively, an agreement, statement of work, or ordering document (as applicable), 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.

"**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) is 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 of a customer, employee, partner, or supplier; intellectual property (IP); source code; passwords; non-personal information concerning Oracle's customers, employees, suppliers or partners; any data stored in or provided from the information systems of Oracle or its customers, employees, suppliers, or partners; and any other Oracle confidential information as defined in the agreement.

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

"facilities" means any offices, data centers and 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. References herein to (i) "Oracle facilities" include facilities of Oracle customers, and (ii) "Supplier facilities" 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 the 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, representatives, and agents who are provided access to Oracle facilities, networks, information systems and/or confidential information.

"**personal information**" means any information to which Supplier is provided access that relates to an identified or identifiable individual, 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.

"security incident" means (a) misappropriation or unauthorized access to or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of confidential information, (b) unauthorized access to information systems, or (c) theft, loss or damage to assets.

"**services**" means the work to be performed by Supplier for Oracle as specified in an agreement.

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

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

APPENDICES (AS APPLICABLE)

Appendix 1: Oracle Supply Chain and High Value Asset Physical Security Standards

Appendix 1: Oracle Supply Chain and High Value Asset Physical Security Standards: 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: Co-Location Security Standard

Appendix 2: Co-Location Security Standard: Applies only to Suppliers who provide 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

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.