ORACLE

Oracle Supplier Information and Physical Security Standards

Effective Date: June 1, 2026

01 June 2026 version
Public

Contents

SCOPE

These Supplier Information and Physical Security Standards and any applicable Appendix (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. The Supplier is responsible for maintaining appropriate technical and organizational measures to safeguard the confidentiality, integrity and availability of confidential information and for the delivery and/or performance of the services as set out in the 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 the agreement, 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 or accessed from, a description of the services performed by such subcontractors, and make that list available to Oracle. 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.

PART B: BUSINESS CONTINUITY AND DISASTER RECOVERY

B.1 Supplier 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 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 Industry and 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.1.2 If Supplier or a Supplier Affiliate will have Access to Oracle or Oracle Affiliates' Covered Data to perform the services, Supplier represents, warrants, and covenants that: (i) neither Supplier nor any Supplier Affiliate who has Access to Covered Data (nor any personnel or subcontractor of Supplier or any Supplier Affiliate who has Access to Covered Data) is a Covered Person; (ii) Supplier and Supplier Affiliates will not engage in any Covered Data Transaction; and (iii) Supplier will immediately notify Oracle in writing if any representation in this Section changes or is no longer true.

D.1.3 If applicable, the Transfer of any Non-Personal Information, including Metadata (both as defined under the EU Data Act), is subject to safeguards as set out in Section 6 of the Oracle Supplier Data Processing Agreement (SDPA).

D.2 Security Compliance and Assessments

D.2.1 If the services include the processing of personal information by the Supplier or personnel, or personal information is otherwise provided to or collected by the Supplier on Oracle's or an Oracle customer's behalf, Supplier must sign an Oracle SDPA.

D.2.2 If the Supplier accesses the Oracle's network, Supplier 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 In the event of a security incident, upon reasonable notice Supplier will coordinate with Oracle and provide access to all information necessary to determine compliance with these Standards and may include a security incident procedure, timelines, root cause analysis, impact assessment, correction actions and mitigation and remediation plans. Supplier shall keep Oracle informed of critical milestones and updates throughout the security incident and remediation.

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. The procedures must include capabilities to detect and analyze security incidents and include reporting, analysis, preservation of evidence, 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 to ensure appropriate procedures are followed for the identification, collection, acquisition, and preservation of information.

E.4 Supplier must report to Oracle Security (Security_Breach_ww_grp@oracle.com) without undue delay and no later than 24 hours any suspected or actual security incident involving Oracle confidential information. Security incidents involving Oracle's services must be reported to Oracle Security within 72 hours. Reports must include any legal requirements to enable Oracle to comply with its mandated reporting requirements.

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. Notification to impacted customers, individuals, and any regulatory authority shall be determined by Oracle in its sole discretion.

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 used to deliver the services.

PART F: IT SECURITY STANDARDS

F.1 IT Security Controls

F.1.1 Supplier's 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 continuously monitor information systems, network devices, applications and services used to deliver services to Oracle, terminate any inactive session 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

systems, network devices, and applications to identify and remediate vulnerabilities and 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. Supplier must also use an independent third party to pentest environments and systems used to provide services or store Oracle confidential information, at least annually, and provide a summary report to Oracle that includes; the environments and systems (i) used to provide services to Oracle or (ii) that process or store Oracle confidential information; findings according to severity; and remediation actions taken or to be implemented.

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 a 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 Supplier's 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's 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 to assist in the identification of the source of an issue and enable a sequence of events to be recreated including, to record when (date and time), who (such as user or service account) and where (IP address/hostname) for all access and authentication attempts and 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 or unauthorized activity and to verify the integrity of the logging process. Supplier must escalate any unauthorized activities according to its documented incident response plan.

F.3.6 On Oracle's reasonable request, depending on the services, Supplier shall promptly provide Oracle access to all relevant logs, generated in connection with the services. Where technically feasible Supplier shall integrate such logs into Oracle's Security Information Event Management (SIEM) platform in accordance with Oracle's reasonable instructions and requirements.

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 for the purposes specified in the agreement, and in compliance with these Standards.

F.9.2 All Oracle confidential information stored at rest, including on Supplier personnel laptop/desktop computers and external electronic media (e.g., USB drive), must be fully encrypted using AES-256-bit encryption. Supplier may not store Oracle confidential information on mobile devices or media cards unless content is encrypted by default, or the devices and media cards are encrypted using AES-256-bit encryption.

F.9.3 Supplier must use secure, encrypted channels (such as TLS 1.2, SFTP, or equivalent) to send bulk data transfers unless an alternative method is approved by Oracle. Supplier will implement integrity checks and restrict access to authorized personnel only.

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, is protected in accordance with the requirements of these Standards, and is promptly deleted 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. Certificates of destruction may be provided to Oracle upon request.

F.9.6 Confidential information exchanged using e-mail must use, Transport Layer Security (TLS) between Oracle mail gateways and Supplier mail gateways which the parties will implement.

F.9.7 Supplier and its personnel will not use personal email accounts for exchanging Oracle confidential information.

F.9.8 Supplier is prohibited from using Oracle confidential information (i) from production systems for development, testing, or staging purposes; and (ii) for deidentifying, pseudonymizing or anonymizing confidential information without express written approval from Oracle as set forth in the agreement, a purchase order, ordering document or statement of work.

F.9.9 Any use of confidential information to train, fine tune, or evaluate artificial intelligence or otherwise evaluate, or improve products or services is strictly prohibited unless expressly authorized by Oracle in a separate written agreement. In the event that Oracle has authorized services that include AI/ML in delivery of the services, Supplier shall ensure that

all AI/ML systems: (a) comply with applicable laws and recognized responsible AI frameworks (e.g., NIST AI RMF, ISO/IEC 42001); (b) do not use any Oracle confidential information, for model training, fine-tuning, or evaluation without Oracle's prior written consent; (c) do not input Oracle confidential information into public or shared AI/ML services without written approval from Oracle; (d) protect the confidentiality, integrity, and availability of Oracle confidential information, applying equivalent security controls to both source data and any outputs containing Oracle confidential information; (e) implement controls to minimize risks of inaccurate, misleading, or harmful outputs; and (f) support input traceability and apply secure development and deployment practices.

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 stored, processed, or 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 is expressly authorized by Oracle personnel.

PART H: DEFINITIONS

The following definitions apply to these Standards:

"**Access**", "**Country of Concern**", "**Covered Data**", "**Covered Data Transaction**", and "**Covered Person**" have the meanings set out under the Final Rule.

"**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity or as otherwise defined in the agreement.

"**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.

"AI/ML Systems" means any artificial intelligence or machine-learning systems, models, services, or tools used by Supplier in delivering services.

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

"Business Continuity" and "Disaster Recovery" ("BCP"/"DR") means the processes, plans, and controls designed to ensure continued delivery of services and protection/recovery of confidential information in the event of disruption, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

"**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.

"**confidential information**" means all Oracle information to which Supplier may be provided 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 Content, Personal Information or Personal Data, or Oracle confidential information as defined in the agreement.

"**deletion**" means permanent and irreversible removal of confidential information from storage media in accordance with industry standards such as NIST SP 800-88.

"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.

"**Final Rule**" means the rule implementing Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, along with any additional guidance, advisory opinions, or licensing decisions, issued by the U.S. Department of Justice.

"**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 or (b) may access, transmit, process or store Oracle confidential information.

"**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, or unauthorized disclosure of confidential information, (b) unauthorized access to information systems, or (c) theft, loss of confidentiality, integrity, or availability or damage to confidential information and 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.

APPENDIX 1 – ORACLE SUPPLY CHAIN AND HIGH VALUE ASSET PHYSICAL SECURITY STANDARDS

A. INTRODUCTION

The successful implementation of the Oracle Supply Chain and High Value Asset Physical Security Standards ("Standards") in this Appendix is dependent upon Supplier and Oracle cooperation and collaboration. However, primary responsibility for the safety and security of Oracle assets remains with Supplier. Supplier must ensure that all affiliated companies and personnel comply with these Standards.

The requirements of these Standards apply globally in all geographical areas. These Standards remain subject to change without notice.

B. WAIVERS

Exception(s) to any of the physical security requirements in this Appendix require a written waiver from an Oracle Global Physical Security (GPS) Executive. To request a waiver, Supplier must submit a written application, including a description of alternative physical security measures that Supplier has or will implement. Oracle GPS will assess whether the alternative physical measures proposed by Supplier are acceptable. If a waiver is granted, it will be effective for no more than one (1) year from the date of issuance, and may be terminated, at any time, by Oracle should there be a change in Oracle business needs, the security risks, or it is found that the Supplier has not adequately implemented and maintained the alternate security measure documented in the waiver request. A granted waiver is effective only for the individual shipments or specific routes and facilities described in the waiver.

C. FACILITY CLASSIFICATION

Security requirements vary depending on the facility category. High Value Product (HVP) is not defined in these standards as it is based on a combination of value and business criticality. Suppliers will be notified if they will be handling HVP:

Category A - Storage/Handling of High Value Product (HVP) for periods in excess of 12 hours. Examples of the type of facility to which this classification applies are:

- Warehousing of HVP in excess of 12 hours
- Repair Vendors-Handling HVP in excess of 12 hours
- Re-manufacture Facilities-Handling HVP in excess of 12 hours

Category B - Storage/Handling of HVP for less than 12 hours. Examples of the type of facility to which this classification applies are:

- Warehousing of HVP for less than 12 hours
- Traditional logistic cross dock operation- (Asset delivered on one vehicle and cross docked onto another vehicle within hours-no storage)
- Repair Vendors-Handling HVP for less than 12 hours
- Re-manufacture Facilities-Handling HVP for less than 12 hours

Category C - Storage/Handling of all other assets for periods in excess of 12 hours. No HVP to be stored/handled in these facilities. Examples of the type of facility to which this classification applies are:

- Warehousing of Non-High Value Assets in excess of 12 hours
- Oracle Services Spare Part Storage Facilities in excess of 12 hours
- Non-High Value Global Stocking Locations in excess of 12 hours
- Non-High Value Repair Vendors/Re-manufacture facilities in excess of 12 hours

Category D - Storage/Handling of all other assets for periods less than 12 hours. No HVP to be stored/handled in these facilities. Examples of the type of facility to which this classification applies are:

- Warehousing Non-High Value Assets for less than 12 hours

- Traditional logistic cross dock operation of non-High Value Assets- (Asset delivered on one vehicle and cross docked onto another vehicle within hours and no storage)

D. PHYSICAL SECURITY STANDARDS BY FACILITY CATEGORY

The following matrix summarizes the physical security standards for each category of facility. More detailed information follows the matrix.

Minimum Security Protection Level

		Category				
	Security Standard	**A**	**B**	**C**	**D**	**Remarks**
	Facility Security					
1.1	Enclosed Building Structure	*	*	*	*	
1.2	Fencing/Gating	*	*	*		
1.3	Exterior Lighting	*	*	*	*	
1.4	24/7 Onsite Security	*				
1.5	Security Check Calls	*				
1.6	Security Officer Procedures	*				
1.7	Duress/Panic Alarms	*	*	*	*	
1.8	Landscaping/ unobstructed view of facility	*	*	*	*	
1.9	All opening that might permit entry, including docks doors, closed and secured when not in use	*	*	*	*	
1.10	Window coverage in storage area	*	*	*	*	
1.11	Access Control System	*	*	*	*	
1.12	Restricted Facility Access	*	*	*	*	
1.13	Photographic Employee Badging Process	*	*	*	*	
1.14	Visitor Badging/Escort Process	*	*	*	*	
1.15	Intrusion Alarm System	*	*	*	*	
1.16	Alarm Response	*	*	*	*	Category A should have 24/7 on-site security and backup procedures should be in place in the event the one site security is unable to respond due to hostage/illness/injury or other events.
1.17	Alarm Transmission Cellular Backup	*	*	*	*	
1.18	CCTV System	*	*	*	*	
1.19	Backup Power for Alarms and CCTV	*	*	*	*	
1.20	Security Technology Regularly Tested	*	*	*	*	
1.21	High Value Area with Access Control/Alarm/CCTV	*	*			
1.22	High Value Stored to Prevent Cross Contamination with Other Customers	*	*	*	*	
1.23	Outgoing Trash Inspected	*	*	*	*	
	Risk Management					

	Fire Safety					
1.24	Fire Alarm System	*	*	*	*	
1.25	Automatic Sprinkler System	*	*			To include Services spare part facility categorized as Tier 1.
1.26	Hot Work & Control of Ignition Sources	*	*	*	*	
	Vehicle Security					
2.1	Container Integrity	*	*	*	*	
2.2	Trailer Integrity	*	*	*	*	
2.3	Hard Bodied Vehicles	*	*	*	*	
2.4	Driver Stops in Designated Areas	*	*	*	*	
2.5	Vehicle Immobilization System	*	*	*	*	
2.6	Communication System	*	*	*	*	
2.7	Pre-Alert High Value Product	*	*			
2.8	Advance Notice of Vehicle and Driver ID checks before departure with assets	*	*	*	*	
2.9	No Pre-loading of trailers. Loading Done in Presence of Driver	*	*	*	*	
2.10	Oracle Freight Only to be opened by Oracle or Customs Officials	*	*	*	*	
2.11	Containers sealed and locked. Seal records retained for 30 days	*	*	*	*	
	Handling Security					
3.1	Handling process sufficient to detect shortages/pilferage, etc.	*	*	*	*	
3.2	Positive verification of shipment integrity at all points of hand off	*	*	*	*	
3.3	Losses reported to Oracle within 24 hours	*	*	*	*	
	Personnel Security					
4.1	Vetting Process/HR Hiring Policy	*	*	*	*	
4.2	Employee Training	*	*	*	*	
4.3	Driver Training	*	*	*	*	

Below are detailed security requirements which should be used in conjunction with the matrix.

1. Supplier Facility Security

- The Supplier is required to provide a secure storage area for Oracle's assets. An enclosed building structure will be used which is designed to deter and prevent unauthorized access.
- Requirement determined by Oracle Global Physical Security (GPS) based on individual facility risk assessment. Fenced facility boundaries, with a perimeter gate or other barrier system that prevents unauthorized access. Access to this area is

only granted after identity and proper authorization are verified. As a minimum the fenced/gated area should encompass the dock area.

- Lighting sufficient to illuminate surrounding property grounds will be provided.
- 24 hours/7days on-site guards are required.
- Regular check calls between on-site guards/officer(s) and their main control centre will be performed.
- Procedures to be in place for Security Officer to take action in the event of an incident.
- Duress/panic alarms for use by lone workers or on-site security. Alarms must be linked to alarm response/law enforcement.
- Landscaping that allows for direct, unobstructed view of the facility from the street and from neighbouring facilities will be maintained.
- All openings that might permit entry, including dock doors, will be closed and secured when not in use.
- Windows in storage areas will be screened with a suitable material to prevent showcasing of assets from outside the building.
- An access control system will be utilized. The system must monitor all openings that might permit entry and be able to track events historically by identity and time of entry/exit. The system should be an electronic access control system. Where this is not employed, Supplier will provide Oracle GPS, the full processes and procedures for the system in use, for review and approval per the waiver process.
- Restricted access into the facility that permits entry only to those given prior authorization to access the facility will be rigidly enforced. This should be in conjunction with any access control system.
- Employee badges are required. A badging process that identifies employees whilst in the facility will be utilised at all badges should include an image of the employee (Photo ID).
- Badges for all visitors are required. All visitors must be escorted within the facility.
- A security intrusion alarm system that covers external doors, including dock doors, into the facility, perimeter openings like skylights, and internal perimeter doors leading to areas storing HVP will be employed. The system will also monitor all vulnerable glass areas and provide an alarm in the event of breakage. Burglar bars or other such physical prevention measure can also be utilized.
- Real-time alarm monitoring and response to the installed security intrusion alarm system will be provided by an alarm response company or a law enforcement Employees should not be utilized as on call first responders to alarm activations out of hours.
- Cellular or similar backup for alarm transmission is required for the facility.
- A closed-circuit television (CCTV) system with coverage sufficient to the capture images of all facility perimeter entry points (doors/windows/skylights etc). The Oracle storage area will be under CCTV coverage at all times to capture all Oracle assets in the facility.
- The CCTV system will record activity 24hours/7day. Where a motion detection system is used it is acceptable for images only to be recorded when movement is detected. Images will be retained for a minimum of 30 days. Where a digital system is not used an individual will be designated as primarily responsible for tape rotation. In circumstances where country Data Protection Laws preclude the retention of images for 30 days or longer, then the local laws will have supremacy. All recording equipment and tapes will be secured in a secure room to which access is restricted to only those responsible for CCTV operation.
- Backup power (such as UPS/generator/battery) will be provided to support the security alarm system and the CCTV system in the event of AC power disruption. The back up power supply must last for at least eight (8) hours. If power is not restored within eight (8) hours then alternate security measures, such as on-site guarding, must be put in place, where this is not already in place.

- All technical security measures including CCTV/Access Control/Alarms will be subjected to regular testing and maintenance where necessary. At least monthly checks of those systems will be performed.
- HVP will be stored in a distinct security storage area. For the purpose of this action, examples of security storage may include sealed or locked containers, locked cages, and locked hard-wall areas. The High Value area will have an auditable access control system, CCTV, and alarms together with the associated back up requirements for the facility systems as a whole.
- Non HVP will be stored in a distinct area to prevent cross contamination with other customer product stored at the facility.
- Outgoing trash will be examined to deter pilferage.

2.Risk Management Facility Fire Safety Requirements

The following facility safety standards are required.

- A fire alarm system will be maintained throughout the area to protect Oracle product. This should send an alarm to a constantly staffed location with staff who are trained to promptly summon the fire department in the event of an alarm.
- Supplier will maintain Oracle product in a facility fully provided with automatic fire sprinklers, which will be in good working order at all times. The sprinkler control valves should be maintained in the open and locked Supplier must inspect the sprinkler control valves using a recorded valve inspection system on a monthly basis.
- Hot Work and Control of Ignition Sources: Supplier shall control ignition sources to prevent a fire exposure to Oracle Hot Work is defined as any operation involving open flames or producing heat or sparks. Examples of Hot Work include cutting, welding, brazing or soldering.

3. Vehicle Security/Assets in Transit

- Container integrity. Prior to stuffing, containers will be inspected to verify the physical integrity of the container structure through a seven-point inspection. (Inspection of: Front Wall, Left side, Right side, Floor, Ceiling/Roof, Inside/outside doors, Outside / Undercarriage)
- Trailer integrity. Prior to stuffing, trailers will be inspected to verify the physical integrity of the trailer structure through a five-point inspection. (Inspection of: Fifth wheel area - check natural compartment/skid plate, Exterior front/sides, Rear bumper/doors, Front Wall, Left side)
- Hard-walled, locked vehicles will be employed during transit for all shipments.
- Drivers shall not deviate from the assigned delivery routes nor make unscheduled Any stops necessary due to local laws regarding driver hours/rest periods will ideally be conducted in secure parking areas. In locations where this is not possible, stops will only be conducted in well-lit recognised stopping areas such as service areas/refuelling stations which are open for business. Stopping in roadside lay-bys, closed service areas/refuelling stations or any other isolated location is prohibited.
- Vehicle immobilization devices will be in place and used when vehicle is stopped and unattended for during driver stops required by local laws or any other reason.
- All Supplier's vehicles used for carrying Oracle assets shall be equipped with a suitable communication system that will allow the vehicle driver to request assistance in the event of an emergency. Routes of the Supplier should be analysed with the possibility of dead spots (for cellular/radio coverage).
    - On a case-by-case merit, Oracle reserves the right to require, at any time, that the Supplier's vehicle tractor units and trailers be fitted with a mutually agreed vehicle location system. Global Positioning System (GPS) is a common term for some type of positioning system. The most common use in freight is a Satellite Tracking System (STS), wherein a vehicle is immediately located by satellite positioning. Where this system is required by Oracle, arrangements must be made to supply Oracle with copies of alarm exception reports when applicable.

- There will be a Pre-Alert for all shipments of HVP alerting both ends as to product, method and route of delivery, and estimated time of delivery. The delivery should be verified by recipient to shipper.
- Supplier must provide advance notification of the driver and vehicle details prior to collection of assets from a warehousing/staging facility. Prior to handing over assets to drivers, checks will be completed on driver's identity via photographic ID to ensure they are the same as the advance notification.
- Loading of Oracle shipments must be done in the presence of the authorized driver, no pre-loading of product shipments on vehicles/trailers for later collection is permitted.
- The Supplier is prohibited from opening sealed packages/boxes etc., unless directed by Customs officials or Any freight showing evidence of being opened or tampered with must be reported to Oracle immediately and a written report is to be produced within twenty-four (24) hours following the discovery. The Supplier must implement procedures for communicating freight discrepancies and damaged cartons to Oracle.
- Supplier's procedures must prohibit unauthorized persons or materials to enter into ocean containers stored or loaded at any facility. At the point of loading/stuffing, all ocean containers loaded with goods must be properly Seals used on all ocean containers bound for the U.S. must meet or exceed the International Standards Organization's Publicly Available Specification 17712 standard for high-security seals. All full (dedicated) trucks and trailers carrying goods from one location to another must be sealed with a tamper- evident seal. Seal numbers must be documented on the truck bill of lading or other applicable transport document.
- Unsealing/Unloading; When transferring or unloading an ocean container, the seal condition and seal number must be verified against documentation at pick-up and/or prior to unsealing/unloading. Records of all seals shall be retained for a minimum of thirty (30) days.
- Shipment discrepancies must be reported to Oracle and the relevant law enforcement agency as is applicable reported as soon as possible. The term "discrepancy" includes pickups or deliveries that differ in piece count, size, or scope from what was expected, and all instances of compromised seal integrity (for example, broken seals, tampered seals, different seal numbers, etc.).

4. Handling Security

- Handling processes sufficient to detect shortage or loss through random procedures will be employed. Procedures will include weighing shipments on calibrated scales, box/cycle counts, signature and time/date requirements at transfer points, proof of inspection by receiver, seal inspection, or sufficient overboxing or wrapping to ensure the integrity of the skid or package.
- At any and every point of cargo hand-off, whether to internal personnel (i.e., truck to distribution center) or subcontractors/agents (i.e., truck to airport), a positive verification of shipment integrity shall occur. Methods can include weight verification, piece count, or other means, but shall include a physical inspection of the freight for damage/pilferage, and hand-over will be recorded by name/agency/signature. These records shall be retained for no less than thirty (30) days and will be made available to Oracle.
- Any losses/shortages identified will be reported to Oracle immediately where possible, but no later than twenty-four (24) Oracle GPS shall have open access to Supplier's facility to conduct audits and loss/theft investigations involving Oracle losses/thefts. Oracle GPS shall, as necessary, participate with Supplier security on investigations and resolutions of issues involving loss/theft investigations. Supplier must notify appropriate law enforcement agency(s).

4. Personnel Security

5The Supplier shall ensure that all employees and sub-contractors including drivers who have access to Oracle assets are favourably vetted before employment commences. Evidence of vetting procedures to be produced at Oracle's request together with the Supplier's human resources hiring policy. Compliance with this section will be governed by existing local laws and regulations.

- All employees will be given training in security vulnerabilities, individual reporting responsibilities, immediate actions to be taken in the event of any security related incident such as robbery or facility take over and internal reporting procedures where theft/pilferage is suspected.
- In addition to above, drivers should be provided robbery and hijacking response training, including what the driver should do in the event of robbery/hijacking while in Training should include the use of any immobilization devices.

E. POINT OF CONTACT

Oracle Physical Security Point of Contact: supplychainphysicalsecurity_ww_grp@oracle.com

APPENDIX 2 – SUPPLIER DATA CENTER/CO-LOCATION SECURITY STANDARD

Purpose

This document applies to Suppliers that provide co-location services (including, without limitation, space, racks, power and cooling) to Oracle. These terms are in addition to the terms of the Oracle Supplier Physical and Information Security Standards (the Standards) and all definitions in the Standards have the same meaning in this Appendix 2.

Additional security requirements, including the production of third-party audit reports and certifications, relating to these services are stated in the agreement or statement of work.

1. Third Party Data Center/Co-Location Site Compliance and Reporting

Throughout the term of the engagement, Supplier will:

- Implement and maintain attestations, certifications and regulatory compliance as listed in the Master Service Agreement (MSA) and/or Statement of Work (SOW).
- Support Oracle's ongoing global compliance effort by providing Oracle with copies of the most recent reports listed in the MSA and/or SOW in a timely manner, to enable Oracle to supply its auditors and customers with compliance documentation and reporting on an ongoing basis.
- Implement and maintain industry-standard IT security assessments for operations at Facilities as listed in the MSA and/or SOW.
- Comply with all local security standards and attestations required by the country in which the data center/co-location facilities are located.
- Maintain the required security controls 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), Protected Health Information (PHI).
- Where applicable, maintain a Business Associate Agreement (BAA) with Oracle, in accordance with the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended, covering the services provided to Oracle.
- Notify Oracle in writing of any material nonconformity identified in any of the reports specified in MSA and/or SOW.

2. Auditing Reporting

This section outlines audit requirements to support Oracle's annual compliance obligations, reporting and certifications.

- Oracle, Oracle's third-party auditors, Oracle's cloud service customers or any regulatory examining authority that has jurisdiction may perform a confidential audit to verify that co-location facilities comply with the standards set forth in the agreement with Oracle. Such audits will have a scope that is limited to a visit to the Facility and/or review of Supplier's standard prepared records in relation to the operation of the co-location facilities.
- Oracle, Oracle's third-party auditors or any regulatory examining authority may perform comprehensive audits of the Facilities, that cover, but are not limited to, the following areas:
    - Physical, administrative, operational, and technical controls for the co-location facility and all associated operations;
    - Procedures to evaluate Supplier's information security and physical security incident management process and response to threats and incidents; and
    - Review operational security policies and Security Standard Operating Procedures (SOP) for the co- location facility.
- For all audits performed under this Appendix:

- Supplier will cooperate with and use commercially reasonable efforts to assist Oracle;
- Will be at no additional cost to Oracle;
- Take place during regular business hours and on a mutually agreed date, time and duration;
- Not have a frequency of more than four times in any consecutive twelve-month period, per location, unless as a result of material changes to services provided to Oracle, or in response to a significant security incident that impacts services; and
- All Third Parties involved in audits will have appropriate confidentiality agreements signed with Oracle.

- Supplier will act promptly to resolve issues and findings and implement recommendations made to address issues identified for specific activities and/or operational areas. Resolution for the most critical findings must be addressed as soon as reasonably possible in light of the severity of the issue and the complexity of the required.
- All issues and findings must be tracked and regular progress reported to Oracle until they are remediated.

3. Co-Location Facility

This section outlines the appropriate and proportionate measures that Oracle requires to protect its assets in co-location facilities against physical and environmental threats. Additional measures may be required due to contractual obligations with Oracle's customers or based upon a physical security risk assessment and will be set forth in the SOW.

3.1 Facility Security

- In accordance with 8.2 of the Payment Card Industry Data Security Standard (PCI DSS), Supplier acknowledges it is responsible for the security of Cardholder Data to the extent that its services impact the security of Oracle's related data environment.
- Facilities must be continuously monitored, staffed, and patrolled by dedicated and qualified onsite security personnel 24 hours a day, 7 days a week, with the goal of preventing, detecting and responding to incidents.
- All entry/exit points to the facility must be monitored 24 hours a day, 7 days a week.
- Primary monitoring of video and alarms must be undertaken by dedicated onsite security personnel located in a restricted/secure space within the facility. All alarms must be responded to immediately.
- Supplier must promptly report (a) incidents such as security breaches, security incidents, death or serious injuries to people or property, and (b) operationally disruptive events within the facility or in the immediate vicinity using a method of communication that is appropriate to the severity of the event. Specific notification SLAs may be listed in the applicable Scope of Work or the ordering document.
- The onsite security team must physically respond within 15 minutes to emergency events, workplace disruptions, and system alarms in relation to services provided to Oracle.
- The onsite security team must maintain electronic or written logs that document all security related events, alarms and patrols. Logs must be maintained in a secure manner and be made available for review upon request by Oracle and/or Oracle auditors.
- Employees at the facility must be provided with training that informs them of their individual responsibilities, safety precautions, how to report suspicious activity or security incidents, and the actions to take in the event of an incident related to security and/or safety.
- Supplier must maintain Standard Operating Procedures (SOPs) for the facility and make them available for review upon request by Oracle and/or Oracle auditors.
- Suppliers accepting deliveries on Oracle's behalf must have procedures in place for documenting receipt and ensuring items are placed in a secured location until Oracle takes possession.

- Photography of Oracle leased spaces is prohibited unless Oracle provides written authorization. Any photography is confidential information..
- A list of site work rules (such as prohibitions on photography, use of mobile devices, safety notices) must be clearly visible at the visitor check-in area, in the local language and in English upon request.
- Segregation for Oracle leased spaces must be achieved by physical barriers, such as solid walls or metal security cages, that extend continuously from the true floor to the true ceiling. The barrier must prevent bypassing above the ceiling or below the floor, regardless of the ceiling or floor height or type.
- All critical site infrastructure must be adequately protected in order to reduce the risks from environmental threats and hazards. Critical equipment must be protected from water leakage damage and monitored via lead detection equipment in critical locations.
- Supporting infrastructure located inside the facility, such as network infrastructure, demarcation points, communications and any other infrastructure used to provide services to Oracle, must have physical security protections to ensure access to those areas is limited to authorized personnel and is monitored.
- Supporting infrastructure located outside the facility, such as generators, cooling towers, fuel tanks, communication lines etc. must have physical security protections to ensure access to those areas is limited to authorized personnel and access is monitored and controlled.
- Supplier must maintain a preventative maintenance program with documented procedures that address critical systems such as UPS, HVAC, generators and fire suppression. Written procedures must be documented, reviewed and published regularly.
- Any proposed changes to the maintenance program and/or testing schedule of all critical systems must be communicated to Oracle in a timely manner and allow for Oracle feedback to address any potential operational disruption.
- The preventative maintenance program schedule and records associated with testing must be made available for review upon request by Oracle and/or Oracle auditors.
- Onsite generators must have fuel capacity that provides at least 48 hours of operational availability when at full. Supplier must also be able to source fuel from a diverse group of suppliers within 18 hours, and provide records demonstrating its ability by, for example, contracts with multiple fuel suppliers.
- Regular testing on each generator must be performed and documented to ensure they operate as expected in the event of disruption to the mains power supplies.
- Backup power must be available to support the alarm system, access control, video systems and other supporting security infrastructure. Where batteries are used as the backup power source, a minimum of 8 hours of power must be available.
- Fire suppression systems must be implemented throughout the facility. Maintenance must be kept up to date in accordance with local requirements and reports must be provided to Oracle and/or Oracle auditors on request.
- The facility must have a central monitor and maintain temperature and humidity within Oracle data halls. Alarms must be automatically generated for any events which exceed environmental thresholds.
- All fire suppression and detection devices must be supported by an independent energy source.
- Access to system or components that allow emergency power shut down must be properly protected from unauthorized or accidental activation.
- Sufficient emergency lighting must be installed and maintained to cover all evacuation routes and emergency exits.

3.2 Facility Access Management

- Prior to granting access to visitors, access to facilities must be confirmed by prearranged appointments, including approval for each visitor. Identities of all authorized visitors must be verified using government issued identification. All visitors must be physically escorted.

- Facility visitor logs must be retained for a minimum of one (1) year and be made available for review upon request by Oracle and/or Oracle auditors.
- Facility personnel and authorized visitors must be issued identification badges/cards. Visitor identification badges/cards must be distinguishable from facility personnel identification. All personnel must display badges at all times when in facilities.
- The facility must be equipped with an electronic, centrally managed access control system. The access control system must record and store entry and exit details for all facility personnel and visitors for at least 90 days.
- Facility specific access cards that are provisioned with access levels will follow a least privileged access model for all personnel.
- Upon termination of employment of facility personnel, Supplier must promptly and within 24 hours remove all access privileges and have badges returned or destroyed and remove all access to systems and facilities and disable accounts.
- Supplier must have a documented chain of custody for any physical keys used to access Oracle leased spaces, storage or other areas. Keys must be locked away and secured and logged in and out. Logs shall be stored for at least one year..
- Keys may not be duplicated or removed from the facility unless authorized by Oracle in writing.

3.3 Business Continuity

- Facility must be served by multiple telecommunications carriers to provide network redundancy.
- Supplier must maintain a formal business continuity plan and/or disaster recovery plan that specifies recovery time objectives for every location where services are provided to Oracle.
- A list of natural and man-made threats specific to the facilities must be included in the BCP/DRP documents, with clear plans that explain how threats are mitigated.
- A hardcopy of the current version of the plan must be located in a secure space within the facility and be made available for review by Oracle and/or Oracle auditors.
- The BCP must be updated and tested on an annual basis. The list of critical personnel and their contact information must be kept up to date.

3.4 Oracle Leased Spaces

- Supplier must not identify, or mark Oracle leased spaces 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.
- Supplier is responsible for ensuring that any person accessing Oracle spaces or assets is specifically authorized by Oracle. Oracle will provide Supplier with a list of approved Oracle employees and vendors that are permitted to have access to the Oracle leased The Supplier must maintain access logs of all personnel entering Oracle spaces with: full name, organization/company name, date and time of entry and exit.
- Supplier or its agents will not enter Oracle’s spaces unless:
    - Has written prior approval from Oracle (which shall include a request by Oracle authorizing individuals from Supplier to perform services within the Oracle Space)
    - Is accompanied by Oracle's representative(s)
    - In case of emergencies, such as fire, water pipe damage, natural disasters etc.
- Oracle will inform Supplier when access must be removed for personnel with access to the Oracle leased spaces. Access must be revoked immediately in the event Oracle informs Supplier to remove access of any Oracle employees, contractors or subcontractors that have access to Oracle leased spaces.

- Access lists for the Oracle leased spaces must be reviewed with Oracle every six (6) months and access removed for personnel who do not require access.
- On request by Oracle and/or Oracle auditors, Supplier must provide access logs and reports to Oracle leased spaces. The logs must contain, at minimum, the following information: Full name, organization/company name, date/time of entry and exit.
- Entry doors to Oracle leased spaces must have two (2) factors of authentication for access, g. using electronic dual identification methods such as PIN pad or biometric scan. Specific information for requirements will be included in the applicable statement of work for the facility.
- Where specified in the statement of work, Supplier must provision and integrate its access control systems and devices with the Oracle access control system.

3.5 Video Surveillance

- The video surveillance system must have coverage sufficient to capture images of all access/egress points to the facility, emergency exits and critical areas such as main distribution points. Cabling associated with security cameras must be protected to prevent tampering or exposure.
- Video must be installed and positioned to capture access/egress points and all surrounding areas leading to all Oracle leased spaces, including storage space and office space. The video must be able to capture identifiable images of all personnel entering Oracle leased spaces.
- The video system must record activity continuously 24 hours a day, 7 days a week. The video system must be continuously monitored by on-site security 24 hours a day, 7 days a week. Video footage must be retained for a minimum of 90 days unless otherwise prescribed by local law.
- Supplier must provide timely access to video to Oracle, upon request.
- Area lighting must be sufficient to support the video system in areas with low lighting and during hours of darkness.
- All video recording equipment and tapes will be stored in a secure area to which access is restricted to authorised personnel only.

APPENDIX 3 – ORACLE SOURCE CODE PROTECTION AND SECURE DEVELOPMENT

This Appendix 3 to the Oracle Supplier Security Standards ("OSSS) 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 apply in addition to the terms of the OSSS and terms used herein but not defined have the meaning in the OSSS. Additional requirements may be included in any agreement.

Part A of this Appendix applies to all Suppliers that access, create, maintain, modify and/or use Oracle source code or hardware design code (together "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.

PART A

1. SECURITY POLICIES AND PRACTICES

Supplier must document, maintain, and apply the following organizational policies and practices which policies and practices shall be provided to Oracle upon request:

- A source code protection policy that states how Oracle source code must be handled and protected across the organization.
- Documented secure coding practices that set forth secure coding and secure by design principles that all developers are required to apply when creating Oracle source code.
- A secure development methodology that is integrated into the Software Development Life Cycle (SDLC) and that:
    - encompasses security principles throughout development and testing, and
    - addresses vulnerability management throughout the SDLC.

2. Secure Development Training

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 SDLC. Upon request, Supplier shall provide Oracle with documentation supporting compliance with training requirements.

3. Software Development Life Cycle (SDLC)

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

- Only authorized personnel may access Oracle source code and only from Supplier-managed devices that meet the security requirements specified in the OSSS and from the authorized locations set forth in the agreement.
- Authorized personnel may only transfer or share Oracle source code with other Supplier employees or individuals who are both, 1) authorized to access or handle Oracle source code and 2) directly involved in the delivery of Supplier's services to Oracle.
- Supplier must use only the highest industry standard transport encryption when uploading or otherwise accessing Oracle source code.
- Supplier must never store or share Oracle source code using non-Oracle approved public/cloud storage/collaboration services.
- Supplier must store Oracle source code in a source code repository. However, while authorized personnel are actively working on Oracle source code, that code may be accessed and temporarily stored on:
    - Supplier's computers (laptops/desktops) located on Supplier's premises, or
    - Oracle-issued laptops on Supplier's premises or at locations specified in the agreement.
    - Removable devices may not be used to store Oracle source code without written authorization from Oracle.

- 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.
- Supplier may only store Oracle source code for as long as it is required and only for the purpose set forth in the agreement. Supplier must securely delete Oracle source code from all computers and devices immediately after the services are completed or terminated. Immediately after the retention period has expired, all Oracle source code in Supplier's possession or control must be permanently and irretrievably deleted from all computers, devices, and backup media. Supplier must promptly provide Oracle a written certification that the Supplier has deleted Oracle source code in accordance with these requirements.
- 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.
- Supplier shall provide Oracle with a list of all embedded open source and licensed source code components that Supplier has included in code delivered to Oracle, including each component's Software Build of Materials (SBOM), or the minimum information required for an SBOM.

PART B

4. Source Code Repository Systems

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

- The manager responsible for the Supplier's services to Oracle must approve individual access to a source code repository containing Oracle source code and the 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 which are required to complete the individual's tasks.
- 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 set out in the OSSS.
- 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 Coordinated Universal 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.
- Individual user accounts must be associated with a single individual. 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, or (iii) completes assigned tasks or otherwise no longer requires access to Oracle source code.
- Supplier must retain Oracle source code repository access and Oracle source code change 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 agreement. Supplier records must be available for inspection by Oracle upon written request.
- The operating system and applications installed to support the Oracle 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 using formal change control procedures.

- Supplier must perform daily incremental backups and weekly full backups of Oracle source code. 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.