ORACLE

Appendix 2: Supplier Co-Location Security Standard

Effective Date: October 2024, Version 1.0

Public

Table of contents

List of tables

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 Information and Physical Security Standards (the Standards) and all definitions in the Standards have the same meaning in this Appendix 2. Additional security requirements relating to these services may be stated in a specified agreement or statement of work.

1. Co-location Site Compliance and Reporting

Throughout the term of the engagement, Supplier will:

1.1 Implement and maintain attestations, certifications and regulatory compliance as listed in TABLE 1.

1.2 Support Oracle's ongoing global compliance effort by providing Oracle with copies of the most recent reports listed in TABLE 1 in a timely manner, to enable Oracle to supply its auditors and customers with compliance documentation and reporting on an ongoing basis.

1.3 Implement and maintain industry-standard IT security assessments for operations at Facilities as listed in TABLE 1.

TABLE 1: Compliance and Auditing Reports

Table 1. Listing of attestations, certifications, and regulatory compliance

Required Report (as applicable, per the statement of work)	**Communication Cadence**
SOC 1 Type 2 Attestation (performed in accordance with SSAE 18 and/or ISAE 3402)	Annual
SOC 2 Type 2 Attestation (performed in accordance with SSAE 18 and/or ISAE 3000)	Annual
SOC 3 Attestation (performed in accordance with SSAE 18)	Annual
ISO 9001: Quality Management	Annual
ISO 50001: Energy Management	Annual
ISO 45001: Occupational Health and Safety Management	Annual
ISO 27001: Information Security Management (Statement of Applicability)	Annual
ISO 14001: Environmental Management	Annual
Information Security Policy	Annual
Regional Business Continuity & Disaster Recovery Plan	Annual
PCI DSS Report on Compliance (ROC) * for onsite review at the co-location site	Annual
PCI DSS Attestation of Compliance (AOC)	Annual
HIPAA Attestation	Annual
FISMA (NIST 800-53)	Annual

1.4 Comply with all local security standards and attestations required by the country in which the co-location facilities are located.

1.5 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).

1.6 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.

1.7 Notify Oracle in writing of any material nonconformity identified in any of the reports specified in Table 1.

2. Auditing and Reporting

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

2.1 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.

2.2 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:

a. Physical, administrative, operational, and technical controls for the co-location facility and all associated operations;

b. Procedures to evaluate Supplier's information security and physical security incident management process and response to threats and incidents; and

c. Review operational security policies and Security Standard Operating Procedures (SOP) for the co-location facility.

2.3 For all audits performed under this Appendix:

a. Supplier will cooperate with and use commercially reasonable efforts to assist Oracle;

b. Will be at no additional cost to Oracle;

c. Take place during regular business hours and on a mutually agreed date, time and duration;

d. 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

e. All Third Parties involved in audits will have appropriate confidentiality agreements signed with Oracle.

2.4 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 remediation.

2.5 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

3.1.1 In accordance with 12.8.2 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.

3.1.2 Facilities must be monitored, staffed, and patrolled 24 hours a day, 7 days a week by dedicated and qualified onsite security personnel with the goal of preventing, detecting and responding to incidents.

3.1.3 All entry/exit points to the facility must be monitored 24 hours a day, 7 days a week, 365 days a year.

3.1.4 Primary monitoring of video and alarms must be undertaken by dedicated onsite security personnel located in a restricted/secure space within the facility perimeter. All alarms must be responded to immediately.

3.1.5 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 other ordering document.

3.1.6 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.

3.1.7 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 assessors.

3.1.8 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.

3.1.9 Supplier must maintain Standard Operating Procedures (SOPs) for the facility and make them available for review upon request by Oracle and/or Oracle assessors.

3.1.10 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.

3.1.11 Photography of Oracle leased spaces is prohibited, unless Oracle provides written authorization in advance. Photography of physical security measures, such as video cameras, access control systems, etc. is not permitted.

3.1.12 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.

3.2 Facility Access Management

3.2.1 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 escorted at all times.

3.2.2 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 assessors.

3.2.3 Facility personnel and authorized visitors must be issued identification badges/cards. Visitor identification badges/cards must be distinguishable from facility personnel identification cards. All personnel must display badges at all times when in facilities.

3.2.4 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.

3.2.5 Facility specific access cards that are provisioned with access levels will follow a least privileged access model for all personnel.

3.2.6 Upon termination of employment of facility personnel, Supplier must promptly and no later than 24 hours remove all access privileges and have badges returned or destroyed, and remove all access to systems and facilities and disable accounts.

3.2.7 Physical keys, such as master keys that provide access to the Oracle leased spaces, storage or office areas must be appropriately managed, locked and kept in a secure area. There must be manual or automated logging that ensures accountability for all use of physical keys. Logging must be retained for one (1) year.

3.2.8 Oracle must be informed if keys are duplicated, replicated and/or prior to keys leaving the facility.

3.3 Facility Access Management

3.3.1 Facility must be served by multiple telecommunications carriers to provide network redundancy.

3.3.2 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.

3.3.3 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.

3.3.4 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 assessors.

3.3.5 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 Facility Access Management

3.4.1 Segregation for Oracle leased spaces must be by physical barriers, such as solid walls or metal security caged area. Segregation must continue below floor and above the ceiling if the floor/ceiling height or type allows the physical barrier to be bypassed.

3.4.2 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.

3.4.3 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 designed to ensure access to those areas is limited to authorized personnel and is monitored.

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

3.4.5 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.

3.4.6 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.

3.4.7 The preventative maintenance program schedule and records associated with testing must be made available for review upon request by Oracle and/or Oracle assessors.

3.4.8 Onsite generators must have fuel capacity that provides at least 48 hours of operational availability when at full load. Supplier must also demonstrate the capability to source fuel from a diverse group of suppliers within 18 hours, by providing evidence of, for example, contracts with multiple fuel suppliers.

3.4.9 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.

3.4.10 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.

3.4.11 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 assessors on request.

3.4.12 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.

3.4.13 All fire suppression and detection devices must be supported by an independent energy source.

3.4.14 Access to system or components that allow emergency power shut down must be properly protected from unauthorized or accidental activation.

3.4.15 Sufficient emergency lighting must be installed and maintained to cover all evacuation routes and emergency exits.

3.5 Oracle Leased Spaces

3.5.1 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.

3.5.2 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 spaces. 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.

3.5.3 Supplier or its agents will not enter Oracle’s spaces unless:

a. Has written prior approval from Oracle (which shall include a request by Oracle authorizing individuals from Supplier to perform services within the Oracle Space)

b. Is accompanied by Oracle’s representative(s)

c. In case of emergencies, such as fire, water pipe damage, natural disasters etc.

3.5.4 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.

3.5.5 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.

3.5.6 On request by Oracle and/or Oracle assessors, 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.

3.5.7 Entry doors to Oracle leased spaces must have two (2) factors of authentication for access, e.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.

3.5.8 Where specified in the statement of work, Supplier must provision and integrate its access control systems and devices with the Oracle access control system.

3.6 Video Surveillance

3.6.1 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.

3.6.2 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 ableto capture identifiable images of all personnel entering Oracle leased spaces.

3.6.3 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 locallaw.

3.6.4 Supplier must provide timely access to video to Oracle, upon request.

3.6.5 Area lighting must be sufficient to support the video system in areas with low lighting and during hours of darkness.

3.6.6 All video recording equipment and tapes will be stored in a secure area to which access is restricted to authorised personnel only.

4. Definitions

Agent: A person or business hired by Supplier to perform work on the Supplier's behalf.

Assessor: A person or business hired to evaluate controls relating to a specific subject matter.

Data Center Auditor: For purposes of this document means Oracle, Oracle's third-party auditors or any regulatory examining authority having jurisdiction over Supplier that participates in an audit.

Data Hall: location within the facility which houses computing and networking equipment owned by Oracle.

Third-party auditor: a person or business who is not an employee of, and not otherwise related to Oracle, hired by Oracle to perform an audit and provide an opinion on the efficacy of controls.

Statement of work/SOW: Detailed agreement between Supplier and Oracle, used to define specific activities, deliverables, pricing, and timelines. Also known as a "service order" or "workorder".

Industry-standard IT security assessments: A common ITevaluation (listed in Table 1) performed by an independent party which describes the security posture of systems or organizations.