ORACLE

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

Effective Date: August 2023, Version 2.0

Public

Table of contents

A. Introduction

The successful implementation of the Oracle Supply Chain and High Value Asset Physical Security Standards in this Appendix is dependent upon Supplier and Oracle working in partnership. However, primary responsibility for the safety and security of Oracle assets lies with Supplier. Supplier must ensure that all affiliated companies and subcontractors utilized by the Supplier also comply with these security Standards.

The requirements of these Oracle Global Supply Chain and High Value Asset Physical Security Standards apply to all geographical areas. The terms in this Appendix 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 Oracle GPS. 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 year from the date of issuance, and may be terminated at any time by Oracle should there be a change in Oracle business needs or the security risks or it is found that the Supplier has not adequately implemented and maintained the alternate security measure proposed in the waiver request. A waiver will be 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 as follows:

Category A - Storage/Handling of HVP for periods in excess of 12 hrs. 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 periods less than 12 hrs. 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 hrs. 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-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. However, backup procedures should be in place in the event the one site security is unable to respond due to hostage/illness/injury or other event.
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 so as 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.

Supplier Facility Security

1.1 The Service provider and/or the sub-contractor 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.

1.2 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.

1.3 Lighting sufficient to illuminate surrounding property grounds will be provided.

1.4 24 hour on-site guarding of facility will be provided.

1.5 Where on-site guarding is provided, regular check calls between officer(s) on site and their main control centre will be performed.

1.6 Procedures to be in place for action for Security Officer to take in the event of an incident.

1.7 Duress/panic alarms for use by lone workers or on site security. Alarms should be linked to alarm response/law enforcement.

1.8 Landscaping that allows for direct, unobstructed view of the facility from the street and from neighbouring facilities will be maintained.

1.9 All openings that might permit entry, including dock doors, will be closed and secured when not in use.

1.10 Windows in storage areas will be screened with a suitable material to prevent showcasing of assets from outside the building.

1.11 An access control system will be utilised. The system must monitor all openings that might permit entry and be able to track events historically by identity and time of entry/exit. Ideally the system will be an electronic access control system. However, where this is not employed the full processes and procedures for the system in use will be provided to Oracle GPS for review and approval.

1.12 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.

1.13 Employee badges are required. A badging process that identifies employees whilst in the facility will be utilised at all times. The badge should include an image of the employee (Photo ID)

1.14 Badges for all visitors are required. All visitors must be escorted within the facility.

1.15 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 high value product 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.

1.16 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 agency. *Effective Date: July 16, 2014*

Employees should not be utilised as on call first responders to alarm activations out of hours.

1.17 Cellular or similar backup for alarm transmission is required for the facility.

1.18 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 to capture all Oracle assets in the facility at all times.

The CCTV system will record activity 24hrs/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 those responsible for CCTV operation.

1.19 Backup power to support the security alarm system and the CCTV system in the event of AC power disruption will be provided. This can be UPS/generator/battery etc. The back up power supply must last for at least 8 hours. If power is not restored within 8 hrs then alternate security measures, such as on site guarding, must be put in place where this is not already in place.

1.20 All technical security measures; CCTV/Access Control/Alarms will be subjected to regular testing and maintenance where necessary. At least monthly checks of those systems will be performed.

1.21 High Value Product 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, 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.

1.22 Non High Value Product will be stored in a distinct area to prevent cross contamination with other customer product stored at the facility.

1.23 Outgoing trash will be examined to deter pilferage.

Risk Management Facility Fire Safety Requirements

The following facility safety standards are required by Oracle Risk Management Department. Any queries by service providers regarding these requirements can be directed to Oracle GPS who will liaise with Oracle Risk Management on the service provider's behalf.

1.24 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.

1.25 Service Providers 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 position. Service Providers agree to inspecting the sprinkler control valves using a recorded valve inspection system on a monthly basis.

1.26 Hot Work and Control of Ignition Sources: Service Providers agree to control ignition sources to prevent a fire exposure to Oracle product. Hot Work is defined as any operation involving open flames or producing heat or sparks. Examples of Hot Work would be cutting, welding, brazing or soldering.

Vehicle Security/Assets in Transit

2.1 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)

2.2 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)

2.3 Hard-walled, locked vehicles will be employed during transit for all shipments.

2.4 Drivers shall not deviate from the assigned delivery routes nor make unscheduled stops. 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/refueling stations which are open for business. Stopping in road side lay-bys, closed service areas/refueling stations or any other isolated location is prohibited.

2.5 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.

2.6 All Service providers, and/or the sub-contractor'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 Service provider's and/or the sub-contractor'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.

2.7 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.

2.8 There will be advance notification of 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.

2.9 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.

2.10 The Service provider and/or the sub-contractor is prohibited from opening sealed packages/boxes etc., unless directed by Customs officials or Oracle. 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 Service provider must implement procedures for communicating freight discrepancies and damaged cartons to Oracle.

2.11 Procedures must be in place to make sure that no unauthorized persons or materials 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 sealed. 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 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.).

Handling Security

3.1 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.

3.2 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 30 days, and will be made available to Oracle.

3.3 Any losses/shortages identified will be reported to Oracle immediately where possible, but no later than 24 hrs. Oracle GPS to have open access to Service provider's and/or the sub-contractor's facility audits and loss/theft investigations involving Oracle losses/thefts. Also, Oracle GPS shall, as necessary, participate with service provider security on investigations and resolutions of issues involving loss/theft investigations. The appropriate law enforcement agency(s) will be notified accordingly.

Personnel Security

4.1 The Service provider 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 service provider's human resources hiring policy. Compliance with this section will be governed by existing local laws and regulations.

4.2 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.

4.3 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 transit. Training should include the use of any immobilization devices.

E. Point of Contact

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