ORACLE

Physical Security, Control, Traceability and Destruction of Supply Chain High Value Assets at External Manufacturers and Suppliers

Document Number and Revision: PROC-10090 Rev 05

Overview

Oracle customers worldwide rely on Oracle solutions to help protect their data, both on premise and in cloud computing environments. As a global company, Oracle takes great care to securely develop, manufacture and distribute its products. Oracle's business partners provide invaluable support to Oracle's global operations. It is therefore critical that Oracle implement processes designed to ensure that Suppliers adhere to Oracle's security standards and practices. Primary responsibility for the safety and security of Oracle Supply Chain and High Value Assets (HVA) lies with the Supplier. The Supplier must ensure that all affiliated companies and subcontractors utilized by the Supplier also comply with these security Standards.

This document outlines the physical security, control, traceability, and destruction of HVA at Supplier sites for Oracle product.

Audience

Suppliers*, Oracle representatives, Facilities and Security personnel, that have a need to be in the secured area to complete their responsibilities.

*- Suppliers translates to External Manufacturers, Joint Development Manufacturer, Original Design Manufacturer, Original Equipment Manufacturer, and Logistic Providers that the Supplier manages.

Contents

ORACLE

1.0 Oracle Physical Security Standards

Facilities that are used to develop, manufacture and distribute Oracle products need to comply with Oracle's Global Physical Security Standards. This includes specific processes and accommodations for High Value Assets. HVA's are defined as hardware that can perform the primary functions, which includes providing instructions, communicating, decode, execute, store data and provide the processing power for the hardware to do its work (be read to or written to) then it's considered to be an option for high value. E.g., PDU, PSU, NICs (Host/Smart), RoT, CPU, Motherboards and select FRUs. As part of the risk assessment when developing a new or updating a part, the engineer responsible must consider the following: Intellectual property, financial factors, technical capabilities, Supply chain (i.e. market constraints, long lead times, ease of counterfeiting, etc.) If a part or assembly contains a part that is designated as an HVA, that part must also be identified and handled as HVA.

Note: Oracle tamper evident labels and appropriate branded packging are considered HVA

The high value asset list is designated by Oracle requirements and therefore is subject to change based on customer or Line of Business (customer and LOB) requirements. If you have any questions on what to consider High Value – contact scosecurityrequest_us_grp@oracle.com.

High Value Assets may contain sensitive instructions and data used in critical operations. Unauthorized access, use, modification, or destruction of HVA's can cause a significant impact to the confidence and integrity of the hardware. Therefore, HVA items require special attention by all involved in the manufacturing, procurement, and handling process.

An assessment will be be completed to ensure the following are in use;

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.
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.
3. Lighting sufficient to illuminate surrounding property grounds will be provided.
4. 24 hour on-site guarding of facility will be provided.
5. Where on-site guarding is provided, regular check calls between officer(s) on site and their main control center will be performed.
6. Procedures to be in place for action for Security Officer to take in the event of an incident.

7. Duress/panic alarms for use by lone workers or on site security. Alarms should be linked to alarm response/law enforcement.
8. Landscaping that allows for direct, unobstructed view of the facility from the street and from neighboring facilities will be maintained.
9. All openings that might permit entry, including dock doors, will be closed and secured when not in use.
10. Windows in storage areas will be screened with a suitable material to prevent showcasing of assets from outside the building.
11. 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. 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.
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.
13. Employee badges are required. A badging process that identifies employees whilst in the facility will be utilized at all times. The badge should include an image of the employee (Photo ID)
14. Badges for all visitors are required. All visitors must be escorted within the facility.
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.
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. Employees should not be utilized as on call first responders to alarm activations out of hours.
17. Cellular or similar backup for alarm transmission is required for the facility.
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 which captures an unobstructed view of all Oracle assets in the facility at all times. Any equipment prohibited should be excluded. Ex. Privacy law, FCC communication, and all other US and local law.
19. 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 90 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 90 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.
20. 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 backup 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.
21. 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.
22. 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. Only high

security locking mechanisms will be used. Oracle recommends digital badge entry systems for efficient tracking of authorizied employees, access times, and badge in attempts. Physical systems using high security locks are permitted. Mechanisms such as bike locks, common padlocks, USB charge locks, doorstop chains and combination locks are not allowed. 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.

23. Non High Value Product will be stored in a distinct area to prevent cross contamination with other customer product stored at the facility.
24. The High Value Area will remain clean and free of food or personal items. Outgoing trash will be examined to deter pilferage.
25. All High Value Material (including RMA, damaged, or defective parts) outside of the High Value storage will remain under the same security constraints as “good” material, regardless of production status.
26. High Value Asset protocols require documented handling processes, including physical inventory list, physical verification of hardware, monitoring CCTV surveillance, tracking of employee access and interactions with the High Value Asset.

2.0 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 direct with Oracle Risk Management on the service provider's behalf.

1. 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.
2. 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.
3. 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.

3.0 Vehicle Security/Assets in Transit

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

4. High Value product shall always maintain Chain of Custody throughout the logistic lifecycle. All high value material require secure storage and shall not be left in trailer overnight.
5. 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 recognized 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.
6. 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.
7. All Service provider's, 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 analyzed with the possibility of dead spots (for cellular/radio coverage).
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. Seals on trailers shall be recorded at loading and at any point where the seal is broken or in any way compromised. Records of all seals shall be retained for a minimum of 90 days.

4.0 Handling Security

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 over boxing or wrapping to ensure the integrity of the skid or package.

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 90 days, and will be made available to Oracle.
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's GPS shall, as necessary, participate with service provider security on investigations and resolutions of issues involving loss/theft investigations.

5.0 Personnel Security

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

6.0 Access Requirements

External Manufacturers and Suppliers must authenticate authorized individuals to the devices and facilities to which access rights are given with a high degree of certainty. In addition, External Manufacturers and Suppliers will enforce access-control policies (e.g., allow, deny, inquire further) consistently, uniformly, and quickly across all resources. Only authorized personnel should request access to the fenced area. When job requirements include a need for access to the secured area, management must review and approve the need for access. Access record retention shall have historical data showing authorized personnel and visitors entering and exiting the secure area. Access to secure area shall be immediately removed upon job rotation or termination.

Approval for access is controlled by External Manufacturing or Supplier's Management, who has control over who will be approved for access to the secured area. The criteria used to determine approval will follow the guidelines below.

1. Requestor is a badged employee with factory floor access
2. Requestor has a legitimate job purpose for being granted access to the secured area
3. Requestor has approval from their immediate manager for access to the secured area

6.1 Exceptions:

Oracle badged employees who have a legitimate job purpose for being in the secured area, but do not have a need for routine access, may enter the area under escort by an authorized employee who has approved access. Access to the secure area shall have historical data of the visitor entering and exiting the secure area.

7.0 Traceability Reporting

Oracle must have the ability to rapidly locate, contain, and replace suspect material throughout the Supply Chain. This capability is referred to as traceability. In this document, as well as in 923-3406, Supplier Traceability Requirements Specification and 7326396, Supplier Traceability Data, CSV Data Feed Format are the requirements and scope of traceability.

Oracle requires all suppliers to provide product traceability and quality data for all products containing Oracle part numbers (PNs) to an Oracle data repository

Traceability provides the following capabilities:

- Proactive customer service before product fails (field change orders)
- Effective control of stop ships, purges, and screens
- Reliable product information capture for development teams
- Greater product and service selling opportunities creation by providing system and component configuration data to the Global Single Instance Install Base (GSI IB)
- Warranty entitlement support
- Verification support of annual failure rate (AFR)
- Ability to trace issues back to the component and supplier level, for example, root cause corrective action (RCCA) and failure analysis (FA)

Traceability benefits are realized not only by Oracle, but by each Oracle supplier implementing component traceability within their own facilities. This enables suppliers to rapidly locate suspect material within their own facilities, hubs, cross docks, and customers.

Oracle expects all suppliers to absorb the costs associated with implementing component traceability, as this provides continuous improvement to their own facilities by realizing cost benefits associated with the capabilities and opportunities described earlier.

The specific Traceability Requirements and Data Transmission Requirements are defined in 923-3406, Supplier Traceability Requirements Specification.

8.0 Destruction of Assets

Specific Oracle Supply Chain High Value Asset (HVA) materials that are determined to be defective, need to be securely destroyed using an Oracle approved secure destruction company. Destruction must be performed the first week of the quarter. Asset list report must be provided to responsible Oracle engineer monthly.

The following actions should be addressed in the Supplier process for managing Oracle's HVAs.

1. Specific part numbers affected will be identified by Oracle through communications to the Supplier.

2. As soon as material is identified as defective, along with supporting evidence to prove so, it is physically segregated from other material to an locked area clearly marked as containing discrepant material.
3. Defective parts are identified/tagged with failure notice or similar method to clearly identify part as non-usable.
4. Defective material must remain or be moved to an inventory location with regular inventory tracking that makes it unavailable (non-netable) for use in manufacturing.
5. All defective parts, including serialized defective parts are identified as defective in the shop floor control system to prevent usage into assemblies. Serialized defective parts such as RoT cards require destruction via shredder to > 10mm.
6. The Supplier will provide quote to Oracle buyer for re-imbursement of the materials costs. (For instances where failure occurs due to supplier control or handling, Oracle will not re-imburse for material costs.)
7. The Oracle buyer will provide a PO to supplier for re-imbursement of material costs.
8. The Supplier will contact the Oracle buyer that is responsible for the part number, provide the contact information for the secure destruction company and the unique identifier of the Technican performing the destruction activity
9. The Supplier is required to screen the secure destruction company for security and quality assurance prior to destroying Oracle material. The supplier is required to notify Oracle upon contractual changes for secure destruction.
10. The Supplier will complete questionnaire provided by the secure destruction company.
11. The Supplier will obtain a quotation from secure destruction company and provide to oracle buyer.
12. Oracle buyer generates purchase order for secure destruction event. Oracle Buyer will coordinate PO creation by country, as needed (e.g.; Oracle Buyer may need to contact other Buyers for PO creation, who are local to country where destruction takes place.)
13. The Supplier will schedule destruction event with approved secure destruction company every quarter. Duration of material stored in secure room shall not exceed the 3 month holding period. The supplier must notify Oracle of the scrapping schedule each quarter. See table for security requirements.
14. The Supplier has oversight of secure destruction event with destruction company, ensuring quantity, part number and serial number accuracy.
15. The HVAs shall maintain chain of custody throughout the destruction lifecycle and shall be destroyed at the site of failure and cannot be relocated offsite for destruction.
16. The Supplier is required to monitor, provide adequate CCTV coverage of the material destruction and retain all recoded material of the event. At a minimum logs detailing the event must be stored for a period of 90 days.
17. The Supplier obtains certificate of destruction (COD) after completion for their records and forwards a copy to Oracle Ops Program Manager. The COD needs to have the following information: date of the destruction activity, the type of activity (shredder, destruction, crusher, etc) the unique identifier of the Technician permforming the destruction. The COD shall incude by line item the part number, brand, qty and each unique serial number.
18. The Supplier maintains each SN record for products destroyed for 3 yrs from date of destruction event.

19. All Oracle material under no circumstances shall be refurbished, repaired, saved, preserved or otherwise reworked for resale, reuse or transfer to another party.

8.1 Destruction of Assets: Security Requirements

Scrapping Requirement	Onsite Degauss and Shred Required
Degauss: 30000	Y
Hard drive disks and tape media: degauss (per above): 2mm - 19mm	Y
HSM Liquid Security Cards (PN 7353797): 2mm - 6mm	Y
All other media (including SSDs PCI Cards- RoT) : 2mm -10mm	Y

9.0 Incident and Change Reporting

The supplier must notify Oracle of significant security change that are likely to effect the security of the facility, hardware and/or line of business. Submit change notice to scosecurityrequest_us_grp@oracle.com

- Change in building modification
- Change in physical security (CCTV, Metal detectors, badge reader, security guards, etc)
- Change in recycler/scrapper selection
- Changes to any processes or procedures that support their Supply Chain Security Operations.

10.0 Contact

For questions, send an email to: scosecurityrequest_us_grp@oracle.com

11.0 Related Information

8218708- Specification for Tamper Evident Packaging

12.0 Document History

REV	DATE	DESCRIPTION OF CHANGE	CHANGE ORIGINATOR
02	05/13/21	Initial Release	N/A
03	10/18/23	Added new requirements for High Value Assets. Listed items within section: Oracle Physical Security Standards - Item 18, 22, 24,25 and 26 Destruction of Assets – Item 2, 4, 5 and 14	N/A

04	5/10/24	Added new requirements for High Value Assets. Listed items within section: Destruction of Assets – Item 5, 8, 9, 14, 15, 16, 17 and 18	N/A
05	7/17/24	Added new requirements for destruction of High Value Assets. Vehicle Security/ Assets in Transit - Item 4 Destruction of Assets - Item 13 Updated definition of High Value Part in 1.0 Oracle Physical Security Standards Added 9.0 Incident and Change Reporting	N/A

When Document Template is complete, email source file to eso_business_docs_us_grp@oracle.com

All hard copies of this document are uncontrolled and are to be used for reference only.