ORACLE

Handling and Disposition of RoT

Document Number and Revision: AQP-10027 Rev 02

Overview

The following requirements apply for supply chain manufacturing of RoT cards supporting NPI & Production.

Audience

SCO, External Manufacturers, Joint Development Manufacturer, and approved 3rd party providers

Table of Contents

1. Impacted Parts

All RoT cards used on Oracle Products

2. Hardware Security Requirements

The following controls are required to provide assurance that RoT cards are safeguarded and accounted for during assembly, rework, upgrade/modifications, and disposal.

- The supplier is required to maintain up-to-date inventory/equipment record providing full physical traceability of the hardware on premise.
- The supplier is required to clearly define the roles and responsibility of all personnel maintaining the accuracy of the hardware, the purchase, transfer and disposition of the hardware.
- All material digitally shop floor and physically transferring in and transfer out will be traced by serial number per PROC-10090 and AQP traceability spec 923-3406.
- Under no circumstances will an item be refurbished, repaired, or otherwise reworked for resale or transfer to another party with or without consideration or compensation.
- No components or any portion of the RoT can be saved or preserved for reuse or resale regardless of whether there is any commercial value in such components.

ORACLE

2.1. RMA

- NOTE: RMA is not standard process. RMA requests are only initiated upon Oracle request.
- Only product with the original Tamper Proof label intact will be eligible for RMA.
- Upon finding, supplier is required to submit non-conforming details for Oracle PE (Product Engineer) to review.
- The submission information must include initial pictures identifying each unique serial number on the card.
- Pictures will be marked with the following “Oracle Confidential- Highly Restricted” and then uploaded through Oracle’s approved secure repository. Contact Oracle PE (Product Engineer) and PM (Program Manager) for instructions.
- Access to the RoT cards will be limited to the authorized personnel.
- Cards are to be stored inside a locked secure room with 24/7 CCTV coverage and full traceability of access in and out of the secure area.
- Daily inventory tracking must be completed. Verification is per the RMA process. The asset serial number match the asset being returned.
- Supplier must submit shipping approval and specify White Glove Service is required.
- Supplier is required to use Tamper Evident label. See 8218708 Specification for Tamper Evident packaging. Contact Oracle PE and PM for instructions.
- Pictures must be provided showing the card SN, showing that the card is in the ESD bag, and the TE label is intact. Picture must be provided to Oracle prior to any hardware leaving premise.
- Supplier will ensure all customer digital data related to RoT are secure and controls are aligned with Information Security Management System policies.

2.2. Secure Transportation Checklist

- RoT Hardware requires formal approval prior to shipment from Hardware Security for rework. Contact scosecurityrequest_us_grp@oracle.com.
- Prior to packing supplier is required to verify serial number against the physical asset.
- Suppliers will not open packaging without Oracle consent and onsite verification when the hardware arrives. Site balance requires an Oracle employee to be onsite.
- Supplier must ensure the storage area is clean and will contain only Oracle material.
- All RoT will be shipped overnight using Oracle approved carrier.
- Chain of custody will be actively monitored to ensure hardware does not sit overnight without the proper security controls.
- High value asset will not be affixed to a location digitally or physically where the hardware loses its traceability and unique identity upon removal or relocation.

2.3. Inspection Upon Arrival

- Site balance requires an Oracle employee to be onsite. Contact PE and PM for instructions.
- Supplier will not open the box until Oracle is onsite for inspection.

- Supplier is required to verify security tamper evident labels are intact and damage/tampering has not occurred. See 8218708 Specification for Tamper Evident packaging inspection requirements.
- Supplier is required to take picture of the asset in its original packaging without opening the package.
- Asset will be labeled to isolate from production material.

3. Destruction of Assets

The following actions will be addressed in the supplier process for managing Oracle's High Value Asset.

Please review Oracle AQP spec PROC-10090.

- Specific part numbers requiring scrapping must be approved by Oracle.
- Supplier must submit the scrap list along with pictures as part of the approval request to Oracle every month via Oracle's approved secure repository, notify PM and PE
- As soon as material is identified as defective, along with supporting evidence to prove failure or non-compliance, it is physically segregated from other material to an locked secure area clearly marked as containing discrepant material.
- Defective parts are identified/tagged with failure notice or similar method to clearly identify part as non-usable.
- 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.
- Must perform onsite destruction the first week of every quarter.
- Supplier must verify that the scrapper:
    - Has certification to an Internationally accepted electronics recycler standard (e.g., R2 - Responsible Recycling Standard for Electronics Recyclers, eStewards - Standard for Responsible Recycling and Reuse of Electronic Equipment).
    - Other industry standards that may apply ISO 9001, ISO 14001 (alternative RIOS), ISO 45001, ISO 27001, OHSAS 18001, ITAD Accreditation, NAID AAA, and ADISA's IT Asset Recovery Certification (UK-developed global standard).
    - Scrapper must demonstrate security practices in the shipment, receipt and processing of electronic waste, and demonstrate environmentally safe handling.
    - Supplier shall audit recycler by standards authority.
    - Final wastes disposed of according to all applicable laws.
    - The scrapper must be compliant with environmental laws, regulations, and ordinances and legal rulings.
- Supplier shall flow Oracle's audit rights to the recycler- Agreement to terms that state, under no circumstances will an item be refurbished, repaired or otherwise reworked for resale or transfer to another party with or without consideration or compensation.
- No components or any portion of an item can be saved or preserved for reuse or resale regardless of whether there is any commercial value in such components.
- Supplier must provide a Certificate of Destruction (COD) along with individualized serial numbers provided for scrapped cards. COD will include:

  - Date of destruction activity
  - Type of activity – Destruction, shredding, etc.
  - Name (or unique identifier) of Technician preforming destruction activity.
  - The COD shall include by line item the part number, brand, qty and each unique serial number.
- 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 2mm-10mm.
- The Supplier will schedule a destruction event with an 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.
- The Supplier has oversight of secure destruction event with destruction company, ensuring quantity, part number and serial number accuracy.
- 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.
- Cards are to be stored inside a locked secure room with 24/7 CCTV coverage and full traceability of access in and out of the secure area.
- 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 log detailing the event must be stored for a period of 90 days.
- 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 performing the destruction.
- The Supplier maintains each SN record for products destroyed for 3 yrs from date of destruction event.

Document History

REV	DATE	DESCRIPTION OF CHANGE	CHANGE ORIGINATOR
02	08/13/2024	Initial Release. Review Ver B: Section 2.1 RMA: - Added a note “RMA is not standard process. RMA requests are only initiated upon Oracle request.” - Added bullet “Only product with the original Tamper Proof label intact will be eligible for RMA.” - Updated SecureSites callout to “Oracle’s approved secure repository” - Updated bullet on photo requirement “Pictures must be provided showing the card SN, showing that the card is in the ESD bag, and the TE label is intact”. Section 2.2 Secure Transportation Checklist:	N/A

		- Removed “outside the United States” in the first bullet. Section 3 Destruction of Assets: - Updated SecureSites callout to “Oracle’s approved secure repository” Review Ver C: fix spelling error and remove bullet – no content changes.	

- 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.
- For questions or comments about this document, please send an email to: eso_business_docs_us_grp@oracle.com