Data Center Security Procedure: Spare Media Preparation and Red Zone Entry

1. Overview

This Procedure defines Spare Media preparation and Red Zone entry requirements for Amazon Data Center Operations, and supports the AWS Media Protection Policy. This Procedure applies to all personnel who access Amazon Data Center sites. Amazon Dedicated Cloud (ADC) facilities, GovCloud facilities, Amazon corporate offices, AWS corporate offices, fulfillment centers, and customer support centers are not within the scope of this Procedure.

2. Definitions

For definitions of terms that are used but not defined in this Procedure, refer to AWS Security's Policy Definitions in Amazon Policy.

2.1. **Red Media:** Any Storage Media that has entered the Red Zone. Any Storage Media discovered in the Red Zone is also classified as Red Media.

2.2. **Spare Media:** Any Storage Media that has not entered the Red Zone is classified as Spare Media. Spare Media does not have the same controls associated with Red Media. Spare Media, in a Yellow Zone, may be stored directly in open inventory bins or within sealed vessels that are checked into inventory bin locations. As with all inventory, the physical location must always match with the logical inventory bin location. Once Spare Media has crossed the Red Zone boundary, it becomes Red Media and is subject to the Data Center Security Standard: Media Handling, Storage and Destruction Standard.

2.3. **Storage Media:** Any electronic device capable of storing customer data to include, but not limited to, Hard Drives (HDD), Solid State Drives (SSD), Tape Cartridges, RAID Cards, USB storage devices, SD Cards, and Compact Flash (CF) Cards.

3. Responsibilities

All Amazon employees and vendors/contractors assigned to use, install, or maintain Amazon information systems must be familiar with this Procedure. Amazon Data Center Security teams establish and enforce this Procedure.

4. Roles

4.1. **Controller:** Amazon Data Center Blue and Green Badge employees.

4.2. **Media Auditor:** Amazon Data Center Blue Badge employees who are members of the Boost-MyDay-Media-Auditor-Role and IAD-Mobility-RAT permission groups. Media Auditors cannot act as a Controller.

4.3. **Security:** Amazon Data Center Yellow Badge Contract Guard Force (CGF) who conduct Clean In Clean Out (CICO) screening at Red Zone entry and exit points. Hereafter, CICO screening checkpoints are referred to Red Zone Entryway Checkpoint (ECP).

5. Requirements

The content in this section describes the specific Procedures that must be enacted and followed by Amazon Data Center personnel in order to meet the requirements of applicable controls. This Procedure must be provided to all Amazon employees and vendors/contractors. All employees must comply with safety requirements defined in the DCGS Safety Standards of Conduct while executing this Procedure.

6. Procedures

Controllers must execute the following Red Zone Preparation Procedures to check out Spare Media into user custody prior to transporting Spare Media to the Red Zone Entryway Checkpoint (ECP). Controllers can opt to transport the Spare Media from the Yellow Zone to the Red Zone utilizing the following sealed or unsealed vessel procedures.

6.1. Spare Media Preparation for Red Zone Entry

6.1.1. Sealed Vessels

The following sealed vessel procedures require a Media Auditor to be present at the time the Controller checks parts into their user custody and does NOT require a serial-level user custody verification scan at the ECP. Instead, the Media Auditor will verify the quantity listed in the 'RZE Preparation Tracker' with the quantity listed in the inventory system as in the Controller's user custody.

6.1.1.1. Controller obtains a vessel that must be clear in hue for transport of Spare Media.

6.1.1.2. Controller obtains tamper-evident, serialized security seals and/or tamper tape (if needed to seal edges).

6.1.1.3. Media Auditor creates an 'RZE Preparation Tracker' by filing a ticket to the site's Data Tech queue utilizing this template.

6.1.1.4. Controller meets Media Auditor at Yellow Zone Spare Media storage location.

6.1.1.5. Controller checks the Spare Media required for their batch into logical user custody, using directed-work or inventory system check out workflows.

6.1.1.6. Controller records all the Spare Media serial numbers placed in the clear vessel in the 'RZE Preparation Tracker' ticket correspondence.

6.1.1.7. Update format:

- **6.1.1.7.1.** Controller: <alias>
- **6.1.1.7.2.** Media Auditor: <alias>
- **6.1.1.7.3.** Sealing drives with serial numbers below in clear vessel with tamper evident seals.
- **6.1.1.7.4.** Quantity:
- **6.1.1.7.5.** Blue Seal #:
- **6.1.1.7.6.** Blue Seal #:
- **6.1.1.7.7.** Mobility Link:
- **6.1.1.7.8.** Serial #s:

6.1.1.8. Media Auditor performs TPVR check of all the Spare Media serial numbers placed in the clear vessel by the Controller in the 'RZE Preparation Tracker' correspondence.

6.1.1.9. Controller seals the clear vessel and updates the 'RZE Preparation Tracker' correspondence with the seal IDs.

6.1.1.10. Media Auditor verifies the vessel seals and updates the 'RZE Preparation Tracker' with the seal IDs.

6.1.1.11. Controller transports the sealed vessel with their Spare Media in user custody directly to the ECP.

6.1.2. Unsealed Vessels

The following unsealed vessel procedures do not require a Media Auditor at the time of inventory check out but does require a, single-piece, serial-level user custody verification scan using the inventory system executed at the ECP by the Media Auditor approving the inventory for Red Zone entry.

6.1.2.1. Controller obtains a vessel that must be clear in hue for transport of Spare Media.

6.1.2.2. Controller moves to Yellow Zone Spare Media storage location.

6.1.2.3. Controller checks the Spare Media required for their batch into logical user custody, using directed-work or inventory system check out workflows.

6.1.2.4. Controller transports the unsealed vessel with their Spare Media in user custody directly to the ECP.

6.2. Spare Media Red Zone Entry

6.2.1. Controller confirms that they have completed the Spare Media Preparation for Red Zone Entry procedures listed above, and that all Spare Media needed for their batch is in physical and logical user custody.

6.2.2. Controller requests Media Auditor presence at ECP.

6.2.3. Controller proceeds with the clear vessel containing Spare Media in their user custody to the ECP.

6.2.4. Media Auditor meets Controller in ECP with a workstation.

6.2.5. Media Auditor locates the site's Red Zone Entry Log.

6.2.5.1. Create a Red Zone Entry Log utilizing this template, after confirming with onsite DCO management, only if there is no existing Red Zone Entry Log ticket.

6.2.6. Security prompts Controller with phrase 'Do you have any media in your custody?' when Controller is attempting to clear through ECP.

6.2.6.1. If Controller responds 'No', but Security suspects custody of media based on what is visually inspected during screening, Security proceeds to escalate appropriately.

6.2.6.2. If Controller responds 'Yes', Security prompts Controller with phrase "Who is your designated Media Auditor?"

6.2.7. Security must not allow access for any employees/contractors attempting to move media into the Red Zone without a Media Auditor present.

6.2.8. Controller provides alias of Media Auditor to Security.

6.2.9. Security verifies Media Auditor from Media Auditor List maintained by the site DCM and DSM.

6.2.10. Controller presents one of the following to Media Auditor:

6.2.10.1. 'RZE Preparation Tracker' and sealed clear vessel containing Spare Media.

6.2.10.2. Individual pieces of Spare Media from their unsealed vessel.

6.2.11. Media Auditor verifies user custody in Mobility for all media inventory presented for Red Zone entry. The Media Auditor will click this Mobility link, and insert the Controller alias into the search field.

6.2.11.1. If the vessel is sealed, the Media Auditor verifies the quantity listed in the user custody inventory search against the quantity listed in 'RZE Preparation Tracker'.

6.2.11.1.1. If the quantity verification is successful, mark "APPROVING RZE for SEAL ID:" and the seal ID.

6.2.11.1.2. If there are discrepancies, the Controller must return to the Yellow Zone Spare Media bin location, rectify inventory scans to reconcile all physical parts in custody match logical inventory records, and repeat the Red Zone Entry Procedure.

6.2.11.2. If the vessel is unsealed, the Media Auditor will click this Mobility link to verify each individual serial number by scanning it validating that the USERNAME listed in the "User Custody" field matches the username of the Controller.

6.2.11.2.1. If any verification fails, the Controller must return to the Yellow Zone Spare Media bin location, rectify inventory scans to reconcile all physical parts in custody match logical inventory records, and repeat the Spare Media Red Zone Entry Procedure.

6.2.12. Once user custody verification for all Spare Media presented to the Media Auditor has passed, the Media Auditor updates 'Red Zone Entry Log' with all serials in user custody, seal IDs (if applicable), and Controller alias.

6.2.13. Update format:

6.2.13.1. Controller: <alias>

6.2.13.2. Media Auditor: <alias>

6.2.13.3. Verified all serials listed below are in user custody at the time of Red Zone Entry. Approving RZE for Seal IDs/Serials listed below.

6.2.13.4. Seal #:

6.2.13.5. Seal #:

6.2.13.6. Quantity:

6.2.13.7. Mobility Link:

6.2.13.8. Serial #s:

6.2.14. Security prompts Media Auditor with phrase "Can you please provide me the ticket?"

6.2.15. Media Auditor provide Red Zone Entry Log ticket number to Security.

6.2.16. Security verifies that the username of the Media Auditor listed in the Red Zone Entry Log, is the username of the Media Auditor physically present at the checkpoint approving Red Zone Entry.

6.2.17. Security verifies that the Media Auditor has updated the Red Zone Entry Log by checking the timestamp at the time of Red Zone Entry.

6.2.17.1. If the Red Zone Entry Log is not updated by the Media Auditor at the timestamp of entry, the Controller must not be permitted to enter the Red Zone with the media.

6.2.18. Security provides update in Red Zone Entry Log "Verified Media Auditor <alias>."

6.2.18.1. If Security identifies a discrepancy with the Media Auditor alias in the log versus the Media Auditor physically present at the ECP, update with "Entry Denied" and the Media Auditor and Controller must restart the Spare Media Red Zone Entry Procedure at the user custody verification at step 6.2.10.

6.2.19. The Controller immediately proceeds through the ECP to the Red Zone with Spare Media in user custody to proceed with their media batch.

6.2.19.1. After physical and logical custody are verified by the Media Auditor at the ECP, the Controller must immediately enter the Red Zone with the Spare Media. The Controller cannot leave the ECP with the Spare Media for any reason, or the Red Zone Entry Procedure must restart.

7. Administrative Information

7.1. Reviews

This Procedure is reviewed and updated annually or as needed, and it is maintained in Amazon Policy.

7.2. Changes

Changes are handled through a defined process, involving three stages: request, approval, and publication. To request a change, visit Data Center Security Procedure Change. After receiving a proposed change, the Data Center Security Policy Manager presents the proposed change (along with a description of the intent) to the owner and relevant stakeholders for approval.

7.3. Exceptions

The requirements outlined in Amazon Procedures are mandatory, and exceptions require explicit written approval. To request an exception, visit Data Center Security Procedure Exception.

7.4. Violations

Violation of this Procedure may result in disciplinary action that may include, but is not limited to, loss of Amazon information resource access privileges, termination for employees and temporaries, and/or restriction from physical access to Amazon data center facilities. To report a violation, visit Data Center Security Procedure Violation.

7.5. Revision History

Version	Version Date	Activity	Author/Participant Alias	Tracking Location (SIM #), Policy Link
0.0	2/11/2022	Draft	Documented in the SIM: 1179	WorkDocs
0.1	2/11/2022	Review and Revision	Documented in the SIM: 1179	Quip
1.0	2/14/2022	Publish	jennijoh	aws-isms-docs-1179
2.0	3/8/2022	Add 6.2.17.	griffend, jeflarso	aws-isms-docs-1179