Data Center Security Standard: Spare Media Handling and Storage

1. Overview

This Standard defines Spare Media handling, storage, and requirements for Amazon Data Center Operations, and supports the AWS Media Protection Policy. This Standard 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 Standard.

2. Definitions

For definitions of terms that are used but not defined in this Standard, 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.

2.2. **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 Standard. Amazon Data Center Security teams establish and enforce this Standard, and ensure that appropriate procedures are established, implemented, and tested in accordance with this Standard.

4. Requirements

The content in this section describes the specific Standard that must be enacted and followed by Amazon Data Center personnel in order to meet the requirements of applicable controls. This Standard must be provided to all Amazon employees and vendors/contractors.

4.1. **Media Deliveries**

4.1.1. At no time shall inbound or outbound media shipments be handled by Yellow Badge personnel. Media shipments will only be handled by Blue and Green Badge personnel.

4.1.2. In a colo, the provider may accept the shipment/media, and store it in their secure storage until DCO comes on site.

4.1.3. Spare Media will be received and recorded in the inventory system of record in accordance with the AWS Data Center Parts Receiving and Exceptions SOP.

4.2. **Preparation and Entry into the Red Zone**

4.2.1. Follow the Data Center Security Procedure: Spare Media Preparation and Red Zone Entry.

4.3. **Loose Media**

4.3.1. If loose media is found in the Yellow Zone (excluding common areas such as hallways, break areas, and other non-office areas), the individual who found the media should immediately notify their direct manager and search the inventory system of record by the media serial number.

4.3.2. If the loose media is recorded as having entered the Red Zone, an immediate notification to Blue Badge Security must take place, and the IRMA process initiated. The person in custody of the media will relinquish control of the media to Blue Badge Security.

4.3.3. If the loose media has no record or has no record of entering the Red Zone, it must be entered into the inventory management system of record and moved into the Red Zone for destruction.

4.4. Inventory Management

4.4.1. Follow the Standard Operating Procedure for Media Cycle Counting for Media Bins and IVTs for cycle counting Spare Media warehoused in inventory locations.

5. Administrative Information

5.1. Reviews

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

5.2. Changes

Changes are handled through a defined process, involving three stages: request, approval, and publication. To request a change, visit Data Center Security Standard 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.

5.3. Exceptions

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

5.4. Violations

Violation of this standard 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 Standard Violation.

5.5. Revision History

Version	Version Date	Activity	Author/Participant Alias	Tracking Location (SIM #), Policy Link
0.0	2/11/2022	Draft and Review	Documented in the SIM	WorkDocs
1.0	2/14/2022	Publish	jennijoh	aws-isms-docs-1178