Data Center Security Standard: Red Zone Laptop Handling

1. Overview

This document provides Amazon data center personnel with a procedure that defines expectations for handling Red Zone Laptops. This procedure supports the Data Center Standard: Clean In, Clean Out (CICO), AWS Media Protection Policy and AWS Physical and Environmental Protection Policy. This document applies to all Amazon data centers participating in CICO.

2. Definitions

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

2.1. **CICO Laptop:** A communal laptop that is deployed for use inside a Red Zone. This laptop is available for use to all persons who have Amazon log in credentials (internal staff and vendors).

2.2. **Mamba:** A global inventory system that tracks the ACME compliance of CICO laptops.

3. Responsibilities

All applicable 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

4.1. Approval Authority

4.1.1. CICO Laptops may enter and exit the Red Zone under the following conditions:

4.1.1.1. CICO Laptops that are deployed in the Red Zone will enter via a CICO Laptop Ingestion Ticket. CICO Laptops are approved centrally by the CICO Global Program Manager (GPM).

4.1.1.2. CICO Laptops that are being deprecated will be removed from the Red Zone via the Red Zone Parts Removal procedure.

4.1.1.3. Employee or vendor laptops for temporary use will enter via a CICO exception. CICO exceptions are approved at the cluster level.

4.1.1.4. Employee laptops entering in support of LSE, CSE, SEV1 or customer impacting SEV2 response will be processed as described in Section 4.8.

4.1.1. Movement of CICO Laptops between Red Zones must comply with the Data Center Security Standard: Secure Handling of Infrastructure Parts (SHIP).

4.2. Escort requirements

4.2.1. All approved vendor laptops that enter a Red Zone must be physically escorted at all times by a Blue Badge employee from the requesting team. Virtual escorts are not permitted in this case.

4.3. Security Seals

4.3.1. CICO Laptops must have security seals applied to cameras before entering the Red Zone and must remain intact throughout the deployment period.

4.3.2. Vendor and employee laptops must have security seals applied to all ports and cameras that are not required for work, and in accordance with the Data Center Security Standard: Clean In, Clean Out (CICO) requirements.

4.3.3. If a security seal shows signs of tampering outside of reasonable wear and tear, such as the anti-tamper label appearing, cluster security must physically isolate the laptop (as prescribed by local cluster security) and conduct a local investigation.

4.3.4. After security seals are applied to a CICO Laptop's camera, DC Security and CGF must conduct weekly inspections to ensure seals have not been tampered with.

4.3.4.1. These inspections must be recorded in an Amazon documentation tool (such as Quip or ticketing) and be available for review upon request.

4.4. Administrator Access

4.4.1. Administrator access on CICO laptops is governed by team rules. If administrator access is required, it must be requested through the AWS RZ ADMIN Team and is limited to 90 days.

4.4.2. The CICO exceptions workflow must not be used to elevate user administrator privileges on vendor or employee laptops.

4.5. USB Functionality

4.5.1. Two separate approvals are required for USB usage in Red Zones.

4.5.1.1. All Amazon laptops are governed by the USB Control Program. If a USB storage device is required for use (USB drive or External Hard Drive), an approval must be in place by an L6 manager submitted via the USB Exceptions Tool.

4.5.1.2. All USB drives entering a Red Zone must be in accordance with the Data Center Security Standard: Media Handling, Storage and Destruction and are require an approved request submitted through the Approval template: 48008.

4.6. CICO Laptop Ingestion

4.6.1. All CICO laptops entering the Red Zone must have the Mamba agent installed and be correctly registered as assets in the Mamba system. Instructions can be found on the Mamba onboarding Wiki.

4.6.2. A CICO Laptop Ingestion Ticket must then be cut with all fields correctly filled out and addressed.

4.6.3. Upon approval, this ticket serves as authorization for brining CICO laptops into a Red Zone.

4.7. CICO Laptop Exception

4.7.1. All laptops entering a Red Zone on a temporary basis (i.e. not a CICO laptop) must have an approved CICO exception.

4.7.2. DC Security must adhere to the global device handling guidance framework when approving exceptions.

4.7.2.1. DC Security approvers must verify that a valid business justification is in place and appropriate mitigations are observed, such as sealing ports and arranging escorts where required.

4.7.2.2. Vendors applying for a laptop exception must have exhausted all prior mechanisms available in the Red Zone before requesting an exception, including using Red Zone laptops, having specific software approved for use via InfoSec, or using a Workspaces account to remotely work in the Red Zone while retaining access to proprietary software.

4.7.2.3. Laptop exceptions may not be approved if requesters have not demonstrated due diligence prior to submitting an approval request

4.8. CICO Laptop Access During Emergency Events in Red Zones

4.8.1. Blue badge personnel may traverse Red Zones with Red Zone laptops.

4.8.1.1. After emergency event resolution, CICO laptops must be returned to their original Red Zone location, and the laptop's make, model, and serial number must be provided to security staff for system recording.

4.8.2. Blue Badge staff who bypassed screening must provide security with the ticket number for the event they responded to, and within 24 hours.

4.8.2.1. Within 24 hours of the bypass, CGF must review the event ticket and verify the responding BB did not create the ticket.

4.8.2.2. Any discrepancies with the even ticket must be immediately escalated to the local security manager for investigation.

4.8.2.3. CGF must inform the local security manager of bypass within 24 hours of the event.

5. Administrative Information

5.1. Reviews

This procedure 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 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.

5.3. 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.

5.4. 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.

5.5. Revision History

Version	Version Date	Activity	Author/Participant Alias	Tracking Location
0.1	5/1/2025	Initial Draft	alexscot	N/A
0.2	5/7/2025	Review and Revision	rissegf, alexscot, nikole	
1.0	7/31/2025	Initial Publication	rissegf, alexscot, nikole	