Data Center Security Standard: Clean In Clean Out (CICO)

1. Overview

This document provides Amazon data center personnel with a standard that defines expectations for implementation of the Clean In Clean Out (CICO) program. This document applies to all Amazon Data Centers participating in CICO. This standard supports the AWS Physical and Environmental Protection Policy.

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. **Clean In / Clean Out (CICO):** The process by which all individuals and objects are screened traversing a Red Zone. The objective of CICO is to protect AWS brand, assets, and proprietary information through enhanced physical security controls of materials entering and exiting Amazon Data Center Red Zones.

2.2. **CICO Approved Tools (CAT):** A central repository that catalogs and tracks tools permitted to enter or exit the Red Zone, distinguishing between those allowed unescorted access and those with associated mitigation requirements.

2.3. **Electronic Device:** An electronic device is any device that can actively or passively perform tasks such as processing, storing, or transmitting information. These devices require a power source and range from simple tools that read, compute, and display data (such as multimeters and basic calculators) to advanced equipment capable of sophisticated data manipulation, storage, and device control (such as computers, smartphones, and specialized equipment like OTDRs).

2.4. **Restricted Items:** Electronic devices (including mass storage media such as HDDs and SSDs) and that require specific authorization for Red Zone entry or exit. Restricted items need local Data Center Security (Blue Badge) approval, while mass storage media and racks must follow prescribed approval frameworks based on the type of movement. Any movement of these items without proper authorization, whether accidental or intentional, is prohibited.

2.5. **Safe Items:** Inert devices without electronic components or data storage capabilities that may freely enter and exit the Red Zone without approvals. These items require no approvals or prescribed mitigations under the CICO Approved Tools program.

2.6. **Screening Checkpoint:** The single, normal means of entry/exit for a Red Zone serving as a transition point where screening operations are conducted.

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

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

4.1. Personnel Screening

4.1.1. All personnel will be subject to mandatory screening when entering/exiting a data center Red Zone. Screening includes metal detection and inspections for prohibited items.

4.1.2. All personnel must stow items not relevant to work prior to entering a Red Zone. Items include but are not limited to wallets, vapes, and knives.

4.1.2.1. All personnel should wear the least volume of metal as practicably possible when transiting a Red Zone.

4.1.2.1.1. This includes plastic/composite alternatives for commonly worn items, such as belts, hair clips, and shoes.

4.1.3. Access to the Red Zone must be denied if an individual fails to pass screening. Denial of access requires escalation to the appropriate security management personnel for review and resolution.

4.1.4. Checkpoint Security Officers accessing the Red Zone to perform screening operations or screening equipment maintenance/calibration do not require screening if they will not cross or access Red Zone areas beyond the delineated screening checkpoint boundaries.

4.1.5. Equipment such as laptops, phones, and radios will be available for use in the Red Zone. Employees and vendors can conduct work within the Red Zone using these shared resources. These items cannot be removed without proper authorization.

4.1.5.1. Personal cell phones are not permitted into the Red Zone for general use.

4.1.6. Exceptional screening and use of prohibited items may be permitted in emergent circumstances (e.g., medical emergencies, law enforcement engagement, natural disasters, power loss). Refer to Data Center Security Standard: Access for Emergency Responders for detailed requirements.

4.2. Checkpoint Configuration

4.2.1. The checkpoint must be a designated area that is physically (i.e. walls, doors) or visually (i.e. stanchions, tape line) delineated.

4.2.1.1. When visually delineated and located inside a Red Zone, the checkpoint boundaries should be located as far as reasonably practicable from deployed servers or racks.

4.2.1.2. Deviations in Screening Checkpoint configuration (i.e. delineation or proximity to deployed servers/racks, must be documented and approved by the CSM and Global Program Manager using Approval Template: 128039.

4.2.2. Security Experience Reporting signage with QR code must be posted in accordance with the Data Center Security Standard: Visual Control Standard.

4.3. Equipment Handling

4.3.1. Cardboard is prohibited from entering the Red Zone.

4.3.1.1.1. Equipment packaging must be removed prior to entering the Red Zone. All equipment trash/garbage must be removed from the Red Zone upon completion of work by the individual(s) who brought the equipment into the Red Zone.

4.3.1.1.2. Cardboard packaging for Nvidia and Annapurna Graphics Processing Units (GPU) is authorized to transit the Red Zone. For detailed screening guidance, refer to the GPU Packaging Guide.

4.3.2. CICO Approved Tools (CAT)

4.3.2.1. Teams must follow the prescribed handling guidance in the CAT catalog when deploying approved tools in the Red Zone.

4.3.2.2. All electronic tools entering and exiting the Red Zone must be processed through Boost Checkpoint.

4.3.2.3. Legacy systems such as Red Zone Passport, Ticketing, or MCM are not permitted without a business justification and an approved exception.

4.3.2.3.1. This excludes ADC and NTE sites, where Boost Checkpoint is not yet deployed.

4.3.2.4. AWS Security and Data Center Security determine the appropriate methods of controls governing tool handling and associated risk.

4.3.2.5. To meet Security Assurance requirements the CAT catalog will be reviewed bi-annually. This audit conforms with NIST MA-3.

4.3.3. Allowed Tools

4.3.3.1. Any item listed in the CAT catalog, power/hand tools, and approved electronic tools are vetted by the CICO GPM and are permitted to enter and exit the Red Zone.

4.3.3.1.1. Each item must follow assigned device handling guidelines and must be reasonably scrutinized and inspected to ensure no prohibited items are concealed within the item.

4.3.4. Device Handling Requirements

4.3.4.1. All battery-powered devices must be powered up at the CICO checkpoint.

4.3.4.1.1. Devices with sealed battery compartments are exempt from battery inspection.

4.3.4.1.2. Devices that cannot power up and cannot have their battery compartment inspected will be denied Red Zone entry.

4.3.4.2. WIFI / Bluetooth capabilities must remain disabled for the duration of the time the device is in the Red Zone, where possible, unless required for work.

4.3.4.3. Devices that require an escort must remain under continuous observation by either a Blue Badge Employee or Contract Guard Force (CGF) while in the Red Zone.

4.3.5. Tool Exceptions

4.3.5.1. If work inside a Red Zone requires an electronic tool that is not on the CAT catalog, a CICO exception must be created. Data Center Security approves each Exception request based on DC security exception guidelines.

4.3.5.2. Exceptions must not be used for operational convenience.

4.3.5.3. Employee laptops may be approved for use under a CICO exception, where a valid business justification exists.

4.3.5.3.1. Vendor laptops may leverage the CICO exception workflow only when all other options, including onboarding vendors to use AWS-owned laptops, have been exhausted and demonstrated to DC Security.

4.3.5.4. Blue-Badge Security Managers must validate that there is no reasonable alternative for the exception and that rigorous mitigating controls are applied.

4.3.6. Hardware and Parts Requirements

4.3.6.1. All hardware and parts intended for use in Red Zones must have approval prior to deployment through either inclusion on the Approved Parts List (APL) for security parts or vetting and approval by AWS-SEC via a Security Workbench Consultation.

4.3.6.2. Hardware and parts must be listed on the Approved Parts List (APL) to be eligible for use in Red Zones.

4.3.6.3. Hardware and parts not listed on mobility with a CSP must undergo a Security Workbench Consultation and receive AWS-SEC approval before deployment in Red Zones.

4.3.6.4. Any hardware or parts exiting the Red Zone must be processed and sanitized, as applicable, in accordance with the associated Component Sanitization Plan (CSP).

4.4. Security Seals

4.4.1. Security seals must be applied to all ports, and compartments, of tools, devices and laptops that transit the Red Zone.

4.4.1.1. Security seals must be non-residue tamper-evident labels.

4.4.1.2. Security seals must be securely stored when not being dispensed.

4.4.1.2.1. Blue Badge Security Managers and specifically trained and delegated CGF personnel are authorized to issue and apply security seals.

4.4.2. Security seals do not have expiration dates and can remain on a device indefinitely once applied.

4.4.3. Exclusions from security sealing include audio and VGA ports, as well as any ports that are required for work inside the Red Zone, which may encompass ports used for data transfer or power delivery.

4.4.4. If a security officer believes a security seal is missing from an item, they are to escalate to a security management for further guidance.

4.5. Photography and Video

4.5.1. Any recording device used must be either on the CAT catalog or approved through CICO exception.

4.5.2. The recording activity must be approved via the Data Center Security Standard: Facility Recording.

4.5.3. Media used during the recording event is governed by the Data Center Security Standard: Media Handling, Storage and Destruction.

4.6. Violations

4.6.1. Any item detected during exit screening that does not have valid transit authority must be reported as a CICO Violation in Resolve.

5. Administrative Information

1.1. Reviews

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

1.2. 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

1.3. 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.

1.4. Revision History

Version	Version Date	Activity	Author/Participant Alias	Tracking, Location (SIM #), Policy Link
0.1	5/7/2025	Initial Draft	rissegf, alexscot, nikole	V1880095491
1.0	7/31/2025	Initial Publication: New document with content pulled from the CICO Procedure in order to streamline standard and procedure content.	rissegf, alexscot, nikole	V1880095491