

Security Boundary

[Go up to Terms and Definitions](#)

Discussion

A Security Boundary is a physical, logical, organizational, or jurisdictional separation between contexts in which different security conditions apply.

The conditions that distinguish one side of a Security Boundary from another may include:

- Governing [Authority](#)
- Applicable [Policies](#)
- Trust assumptions
- Security classifications
- Access-control rules
- Identity and authentication requirements
- Information-release criteria
- Data-handling restrictions
- Monitoring and audit requirements
- Permitted information flows

A Security Boundary does not need to correspond to a physical perimeter. It may occur between Systems, components, networks, organizations, [Jurisdictions](#), trust contexts, classification levels, or processing environments.

Structured information crossing a Security Boundary may require authorization, validation, filtering, transformation, release, rejection, recording, or other security controls. The applicable controls are determined by the Authorities and Policies governing the boundary and the information being exchanged.

A Security Boundary is distinct from an authorization boundary. An authorization boundary identifies the System components included within a particular security authorization. A Security Boundary identifies a change in the security conditions governing an interaction or information flow.

Definition

a physical, logical, organizational, or jurisdictional boundary across which the applicable security Authority, Policies, trust assumptions, classifications, access controls, or information-handling constraints differ

Source

Informed by the [<https://csrc.nist.gov/glossary/term/boundary>|NIST definition of Boundary] and

specialized for structured information processing across governed security contexts in Dido Solutions specifications.

Note

Crossing a Security Boundary does not itself authorize an information exchange. The applicable Authorities, Policies, Interface Contracts, and security controls determine whether the exchange is permitted and what processing must occur at the boundary.

Multiple Security Boundaries may exist within one organization or Jurisdiction. A single Security Boundary may also separate Systems operated by different organizations or Jurisdictions.

Example

A logistics System operating in a classified environment sends an approved subset of supply-status information to an unclassified coalition System. Differences in classification, access rules, release Authority, and information-handling requirements establish a Security Boundary. The crossing applies the authorized filtering, validation, release, and recording controls before the information enters the receiving environment.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:
https://wiki.didosolutions.com/public/99_annexes/annex-b-terms-and-definitions/s/security_boundary

Last update: **2026/09/14 14:18**

