Information Handling Rules

Go up to Terms and Definitions

Discussion

Information Handling Rules are requirements and constraints governing how information is marked, accessed, used, stored, processed, reproduced, transmitted, transferred, retained, archived, downgraded, declassified, or destroyed.

Information Handling Rules can derive from:

- A Security Classification
- A Classification Authority
- Compartments
- Handling caveats
- Dissemination restrictions
- Legal obligations
- Regulatory obligations
- Contractual obligations
- Organizational policy
- Privacy requirements
- Export-control requirements
- Intellectual-property restrictions
- Mission policy
- Records-management requirements

Information Handling Rules can govern:

- Classification and control markings
- Identity requirements
- Authentication requirements
- Authorization requirements
- Need-to-know requirements
- Permitted roles
- Permitted recipients
- Permitted Security Domains
- Permitted Infrastructure Environments
- Permitted Deployment Targets
- Storage protections
- Processing restrictions
- Transmission protections
- Cryptographic requirements
- Media controls
- Reproduction restrictions
- Printing restrictions
- Import controls
- Export controls

- Release conditions
- Transfer approval
- Retention periods
- Archival requirements
- Downgrading requirements
- Declassification requirements
- Sanitization requirements
- Destruction requirements
- Audit and Evidence requirements

Information Handling Rules can apply to:

- Individual information objects
- Collections of information
- Artifacts
- Machine Images
- Infrastructure Baselines
- Configuration records
- Deployment records
- Dependency records
- Evidence
- Metadata
- Aggregated information

Information Handling Rules can depend on both the information and its context.

For example, the rules governing an Artifact can depend on:

- Its Security Classification
- Its compartments and caveats
- Its origin
- Its intended recipient
- Its current Security Domain
- Its destination Security Domain
- Its transfer mechanism
- Its retention status
- Its release authorization

A Cross-Domain Transfer must enforce the Information Handling Rules governing the information, source Security Domain, destination Security Domain, and transfer mechanism.

Definition

requirements and constraints governing the permitted handling of information throughout its lifecycle

Source

- Executive Order 13526, Classified National Security Information
- 32 CFR Part 2001, Classified National Security Information
- 32 CFR Part 2002, Controlled Unclassified Information
- NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations
- Dido Solutions, Crucible architecture and requirements terminology

Note

Information Handling Rules are not limited to classified information.

Unclassified information can require handling controls because of:

- Controlled Unclassified Information requirements
- Privacy obligations
- Export controls
- Contract restrictions
- Proprietary-information protections
- Records-management obligations
- Mission restrictions

Information Handling Rules differ from a Security Classification:

- A Security Classification identifies a protection level or classification designation
- Information Handling Rules identify the actions, restrictions, and controls required for the information

Information assigned the same Security Classification can have different Information Handling Rules because of different compartments, caveats, release restrictions, origins, or mission constraints.

Example

Information classified as Secret has handling rules requiring:

- Secret markings
- Access only by authorized personnel with a need to know
- Storage within an authorized Classified Environment
- Encryption during authorized electronic transmission
- Transfer only through an approved Cross-Domain Transfer mechanism
- Preservation of transfer Evidence
- Destruction through an approved destruction process

Additional compartment restrictions can further limit the permitted recipients and destination Security Domains.