

Unclassified Environment

[Go up to Terms and Definitions](#)

Discussion

An Unclassified Environment is an operating environment that is not authorized to store, process, or transmit classified information.

An Unclassified Environment can still require security controls for information that is sensitive, regulated, proprietary, private, mission-critical, or subject to safeguarding or dissemination restrictions.

Information handled within an Unclassified Environment can include:

- Public information
- Internal organizational information
- Proprietary information
- Personal information
- Export-controlled information
- Law-enforcement-sensitive information
- Controlled Unclassified Information
- Information subject to contractual restrictions
- Information subject to statutory or regulatory protection
- Security configuration information
- Authentication and authorization information

The designation **Unclassified Environment** does not mean:

- The environment contains only public information
- The environment requires no security controls
- Every user can access every resource
- Information can be released without authorization
- The environment can accept classified information
- The environment has a low security-impact categorization

An Unclassified Environment can operate as a:

- [Connected Environment](#)
- [Disconnected Environment](#)
- [Air-Gapped Environment](#)

Connectivity and classification describe different environment characteristics. An Unclassified Environment can remain disconnected or air-gapped because of operational, privacy, export-control, safety, intellectual-property, or cybersecurity requirements.

Within the Crucible architecture, an Unclassified Environment can contain one or more [Deployment Targets](#). Each Deployment Target record should identify the information-handling restrictions, security controls, and authorizations governing that target.

Definition

operating environment that is not authorized to store, process, or transmit classified information

Source

- [Executive Order 13526, Classified National Security Information](#)
- [32 CFR 2002.4, Definitions](#)
- Dido Solutions, Crucible architecture and requirements terminology

Note

Unclassified information can still require safeguarding and dissemination controls.

Controlled Unclassified Information is unclassified information subject to controls established by law, regulation, or government-wide policy. Controlled Unclassified Information is not a Security Classification.

An Unclassified Environment can have a high security-impact categorization based on the consequences of unauthorized disclosure, modification, disruption, or destruction. Security classification and security-impact categorization serve different purposes.

An Unclassified Environment differs from a [Classified Environment](#):

- An Unclassified Environment is not authorized to handle classified information
- A Classified Environment is authorized to handle specified classified information

Information does not become unclassified merely because it enters an Unclassified Environment. Classified information introduced into an Unclassified Environment constitutes a security incident and remains subject to the governing classification authority.

Example

An Air-Gapped Deployment Target hosts Controlled Unclassified Information but is not authorized for classified information.

The Deployment Target remains an Unclassified Environment even though it requires:

- Restricted physical access
- Multifactor authentication
- Role-based authorization
- Encrypted storage
- Controlled media transfer
- Audit logging
- Approved software repositories

- Information-retention controls
 - Information-destruction procedures
-

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

From:

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

Permanent link:

https://wiki.didosolutions.com/dido/99_annexes/annex-b-terms-and-definitions/u/unclassified_environment

Last update: **2026/07/22 13:22**

