

Confidentiality

[Go up to Terms and Definitions](#)

Discussion

Confidentiality protects [Information](#) against unauthorised availability or disclosure.

Confidentiality controls restrict access according to the information's classification, applicable [Policy](#), authorised purpose, and the identity or role of the requesting person, organisation, process, or [Node](#).

Controls supporting Confidentiality include encryption, [Authentication](#), [Access Control](#), information minimisation, redaction, segregation, and protected storage and communication.

Confidentiality remains distinct from [Integrity](#). Confidentiality concerns unauthorised availability or disclosure. Integrity concerns accuracy, completeness, and protection from unauthorised alteration.

Definition

property of information that restricts its availability and disclosure to authorised individuals, entities, and processes

Source

Adapted from ISO/IEC 27000, Information security, cybersecurity and privacy protection — Vocabulary.

Note

Confidentiality applies throughout the information lifecycle, including creation, processing, transmission, storage, use, archival, and disposal.

Confidentiality does not require secrecy for all information. The applicable controls reflect the information's classification, purpose, applicable policy, and consequences of unauthorised disclosure.

A protected record uses a reference, identifier, digest, token, or redacted representation when reproducing the original value would violate its confidentiality controls.

Example

Encryption and Access Control preserve the Confidentiality of a private cryptographic key by limiting its disclosure to authorised processes.

© 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/c/confidentiality

Last update: **2026/08/08 12:58**

