Confidentiality or non-disclosure agreements

ISO 27002 Control 6.6

Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties

Purpose

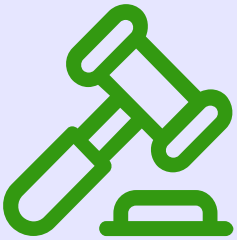
To maintain confidentiality of information accessible by personnel or external parties

Why is it important?

- CDAs/NDAs protect the organization's information and assets (including trade secrets and IP) using legally binding terms
- They clearly inform signatories of their specific responsibility to protect, use, and disclose information in an authorized manner

How to implement it?

- Identify, document, and require relevant parties to sign CDAs/NDAs
- Determine the terms based on the type, classification level, and permissible use of information
- Regularly review the agreements periodically and when changes occur that influence the requirements
- Ensure compliance with the jurisdiction to which the agreements apply
- Agreements should be reviewed periodically and when changes occur that influence requirements



What are the main concepts behind it ?

- Confidentiality or non-disclosure agreements (CDAs/NDAs)
- Confidential information
- Intellectual property
- Legal enforceability
- Jurisdiction compliance

Link with other frameworks

- NIST 800-53 rev5 : PS-6
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting