

Terms and conditions of employment

ISO 27002 Control 6.2

Control

The employment contractual agreements should state the personnel's and the organization's responsibilities for information security

Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered

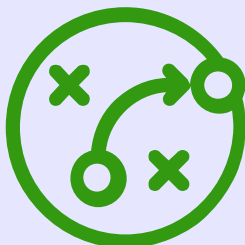


Why is it important?

- Contractual obligations help enforce compliance with security policies and relevant laws (copyright, data protection)
- Ensures continuity of protection for assets and confidential information after employment ends

What are good attributes ?

- Employment contract
- Responsibilities for information security
- Copyright and data protection
- Classification of information
- Penalties for non-compliance
- Acceptance of annexes to the employment contract or code of conduct



What can go wrong if badly implemented ?

- Personnel being unaware of their specific security obligations based on their access level
- Legal or contractual liabilities due to failure to clarify responsibilities (e.g., regarding copyright)
- Lack of enforcement mechanisms if personnel disregard security requirements
- Applying it only to permanent employees (they apply to all personnel, and equivalent agreements should be considered for non-legal entities)

Link with other frameworks

- NIST 800-53 rev5 : PL-4, PS-6
- NIST CSF 2.0 : PR.DS-01, PR.DS-02, PR.DS-10



Renaud Dardenne
Asphalia Consulting