Responsibilities after termination or change of employment

ISO 27002 Control 6.5

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties

Purpose

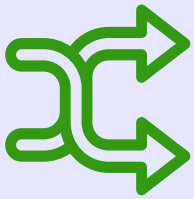
To protect the organization's interests as part of the process of changing or terminating employment or contracts

Why is it important?

- It prevents unauthorized disclosure of confidential information or IP after an individual leaves
- It ensures the continuity of information security management by transferring essential roles to another individual
- Responsibilities contained in terms of employment should continue for a defined period after the end of employment

How can it be implemented ?

- Define, enforce, and communicate responsibilities that remain valid post-termination or change (e.g., confidentiality, IP)
- Manage changes of responsibility or employment as the termination of the current responsibility combined with the initiation of the new one
- Identify and transfer information security roles held by the individual



How is it be proved ?

- Documented list of security responsibilities and duties remaining valid post-termination (often included in employment terms 6.2)
- Records of information security roles being transferred to another individual
- Documented communication process for communicating changes to relevant parties

Link with other frameworks

- NIST 800-53 rev5 : PS-4, PS-5
- NIST CSF 2.0 : GV.RR-04, PR.DS-01, PR.DS-02, PR.DS-10

Renaud Dardenne
Asphalia Consulting