Disciplinary process

ISO 27002 Control 6.4

Control

A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation

Purpose

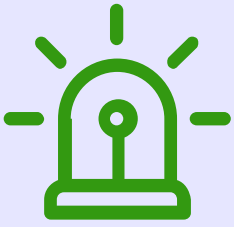
To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation

Why is it important?

- It ensures violations are addressed formally and consistently
- The process serves as a deterrent to prevent future information security policy violations
- It ensures actions comply with applicable legal and contractual requirements

What is a good disciplinary process ?

- Defined and communicated
- Gradual, progressive
- Definition of the seriousness of the violation
- Definition of intentionality
- First offence or repeat offence
- Applicable for security violations



What could go wrong ?

- Inappropriate action taken without verification
- Legal non-compliance if statutory requirements are ignored
- Lack of deterrence leading to repeated violations
- Inconsistent responses based on severity or intent
- Immediate termination is not always the necessary action (the process requires a graduated response based on analysis)
- Do not initiate the process without prior verification that a policy violation has occurred

Link with other frameworks

- NIST 800-53 rev5 : PS-8
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting