

Checklist

5.18 – Toegangsrechten

Thema: Organisatorisch | ISO 27002: 5.18 | Gerelateerd: 8.2, 8.3

Doelstelling

Aantonen dat toegangsrechten tot informatie en systemen worden verleend, beheerd en ingetrokken op basis van vastgesteld beleid en de principes van least privilege en need-to-know.

Beleid voor toegangsrechten

- ☐ Is er vastgesteld beleid voor het verlenen en beheren van toegangsrechten?
- ☐ Zijn de principes van least privilege en need-to-know formeel vastgelegd?
- ☐ Is het beleid van toepassing op alle gebruikers, inclusief beheerders en tijdelijke medewerkers?
- ☐ Wordt het toegangsbeleid minimaal jaarlijks herzien?

Verlening van toegangsrechten

- ☐ Is er een formeel aanvraag- en goedkeuringsproces voor toegangsrechten?
- ☐ Worden toegangsrechten alleen verleend na expliciete goedkeuring van de leidinggevende?
- ☐ Worden toegangsrechten vastgelegd in een autorisatiematrix?
- ☐ Is er scheiding van functies (segregation of duties) toegepast voor kritieke processen?
- ☐ Worden tijdelijke toegangsrechten voorzien van een verloopdatum?

Wijziging en intrekking

- ☐ Worden toegangsrechten direct aangepast bij functiewijziging?
- ☐ Worden toegangsrechten direct ingetrokken bij uitdiensttreding (liefst geautomatiseerd)?
- ☐ Is er een offboarding-checklist die toegangsintrekking afdwingt?
- ☐ Worden accounts van vertrokken medewerkers geblokkeerd en na retentietermijn verwijderd?

Periodieke review

- ☐ Worden toegangsrechten minimaal jaarlijks gereviewed door proceseigenaren?
- ☐ Worden overtollige rechten na review direct ingetrokken?
- ☐ Zijn reviewresultaten gedocumenteerd en aantoonbaar opgevolgd?



Worden afwijkingen gerapporteerd aan de CISO of beveiligingsfunctionaris?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.