

Checklist

8.2 – Toegangsrechten

Thema: Technisch | ISO 27002: 8.2 | Gerelateerd: 8.1, 8.3, 8.5

Doelstelling

Aantonen dat toegangsrechten tot informatiesystemen, applicaties en gegevens op gecontroleerde wijze worden verleend, beheerd, herzien en ingetrokken — op basis van het 'need-to-know' en 'least privilege' principe.

Verlening van toegangsrechten

- ☐ Is er een formeel proces voor het aanvragen en goedkeuren van toegangsrechten?
- ☐ Worden toegangsrechten alleen verleend op basis van een aantoonbare taak/rol (need-to-know)?
- ☐ Is voor elke toekenning een autorisatie van een verantwoordelijke leidinggevende vereist?
- ☐ Worden toegangsrechten vastgelegd in een autorisatiematrix of vergelijkbaar systeem?
- ☐ Wordt het 'least privilege' principe gehanteerd (minimale rechten nodig voor de taak)?

Beheer van toegangsrechten

- ☐ Worden toegangsrechten bij functiewijziging direct aangepast?
- ☐ Worden toegangsrechten bij uitdiensttreding direct ingetrokken (liefst geautomatiseerd)?
- ☐ Is er een proces voor tijdelijke toegangsrechten met een verloopdatum?
- ☐ Zijn gedeelde accounts en generieke accounts verboden of expliciet beperkt?
- ☐ Worden speciale (beheers)rechten apart beheerd en beperkt tot noodzakelijke personen?

Periodieke review van toegangsrechten

- ☐ Worden toegangsrechten minimaal jaarlijks gereviewed door de proceseigenaar?
- ☐ Zijn de uitkomsten van de review gedocumenteerd en bewaard?
- ☐ Worden overtoollige of niet meer benodigde rechten na de review direct ingetrokken?
- ☐ Worden ongeautoriseerde afwijkingen op toegangsrechten als beveiligingsincident behandeld?

Speciale toegangsrechten (privileged access)

- ☐ Zijn beheerdersrechten (admin/root) beperkt tot een minimale groep medewerkers?
- ☐ Worden beheerdershandelingen gelogd en gemonitord?

- ☐ Wordt gebruik gemaakt van aparte beheerdersaccounts (niet het dagelijkse gebruikersaccount)?
- ☐ Is er een procedure voor noodtoegang (break-glass) met logging en nacontrole?

Logging en detectie

- ☐ Worden inlogpogingen en toegangsacties gelogd?
- ☐ Worden logs bewaard conform de retentiebeleid van de organisatie?
- ☐ Worden afwijkende inlogpatronen actief gemonitord (SIEM of vergelijkbaar)?
- ☐ Is er een procedure voor opvolging bij gedetecteerde afwijkingen?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na functiewijziging ☐ Na incident	Status:	☐ Voldoet ☐ Actiepunt ☐ N.v.t.