

Digitale Leveranciers: Zo Houden We Het Veilig

Deze infographic beschrijft de procedure voor het beheren van leveranciers van software, clouddiensten en hardware. Het doel is om de veiligheid, integriteit en continuïteit van onze digitale middelen en diensten te garanderen.

1. Intake & Selectie



Controleer de software op de Softwarecheck-pagina en bepaal het basisrisico.

2. Toetsing & Besluit



Risico's worden beoordeeld (o.a. via verwerkers-overeenkomst); alleen bij acceptabel risico volgt goedkeuring.

3. Vastlegging



De leverancier wordt opgenomen in het dataregister en de Softwarecheck-pagina (groen/rood).

4. Periodieke Beoordeling



De controller voert minimaal jaarlijks een controle uit op risico's en afwijkingen.

5. Beëindiging & Exit



Bij het einde van het contract wordt veilige dataverwijdering en bewijs hiervan geregeld.

Rollen & Verantwoordelijkheden



Schooldirecteur / Domeinbeheerder

Melden van nieuwe of gewijzigde digitale leveranciers bij de Privacy Officer.



Privacy & Security Officer

Controleren van overeenkomsten, beoordelen van risico's en adviseren van het CvB.



Controller

Uitvoeren van de jaarlijkse beoordeling van de (midden-hoog risico) leveranciers.



College van Bestuur (CvB)

Eindverantwoordelijk; keurt overeenkomsten met hoge risico's definitief goed.