Agendapunt
voor de vergadering van het algemeen bestuur Omgevingsdienst Drenthe
2 juli 2026

Datum: 18 juni 2026 Opsteller: M. van den Berg M. Heidekamp-Prins, directeur Omgevingsdienst Drenthe	
Openbaar: Ja	
Advies eigenarenoverleg: Het eigenarenoverleg adviseert in te stemmen met het gevraagde besluit.	
Onderwerp	Cyberbeveiligingswet (Cbw) – duiding en vervolgstappen voor de organisatie
Gevraagd besluit: 1. Kennis te nemen van de Cyberbeveiligingswet, de verantwoordelijkheidsverdeling en de gevolgen voor de organisatie; 2. In te stemmen met het uitvoeren van een impactanalyse en het opstellen van een plan van aanpak.	
Inleiding	De Cyberbeveiligingswet (Cbw) is de Nederlandse omzetting van de *Europese Network and Information Security directive* (NIS2-richtlijn). De NIS2-richtlijn is gericht op het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten. Deze verbetering is noodzakelijk vanwege meer afhankelijkheid van digitalisering en toegenomen dreigingen. Omgevingsdienst Drenthe valt onder de reikwijdte van de Cyberbeveiligingswet (Cbw / NIS2). Deze wet brengt aanvullende verplichtingen met zich mee op het gebied van cyberrisicobeheer, incidentmelding en bestuurlijke verantwoordelijkheid. In dit agendapunt wordt u geadviseerd om kennis te nemen van de gevolgen van de Cyberbeveiligingswet voor de organisatie en de bestuurlijke verantwoordelijkheden zoals beschreven. Om de impact in beeld te brengen wordt voorgesteld om een impactanalyse op te stellen en deze uit te werken in een plan van aanpak.
Motivatie	*1.1 Inwerkingtreding verwacht in 2026, OD's onder reikwijdte* De Cyberbeveiligingswet (Cbw) treedt naar verwachting in het tweede kwartaal 2026 in werking. Het doel van deze wet is om de digitale weerbaarheid van organisaties te versterken. Omgevingsdiensten vallen ook onder deze wet en dienen te voldoen aan verplichtingen op het gebied van risicobeheer, beveiligingsmaatregelen en incidentmelding. Hiermee wordt cyberweerbaarheid nadrukkelijk een bestuurlijke verantwoordelijkheid. *1.2 Uitvoering onder verantwoordelijkheid van dagelijks bestuur* De wet heeft gevolgen voor de inrichting van informatiebeveiliging binnen de organisatie. Het dagelijks bestuur is verantwoordelijk voor de implementatie en naleving en dient zorg te dragen voor passende

	maatregelen, middelen en capaciteit. Het Algemeen Bestuur houdt toezicht en wordt periodiek geïnformeerd over risico's en voortgang. *1.3 Wat vraagt mogelijk extra inzet naast huidige BIO-maatregelen* De bestaande BIO-maatregelen (Baseline Informatiebeveiliging Overheid) vormen het uitgangspunt, maar aanvullende inzet kan nodig zijn, onder andere voor risicoanalyses, audits en externe toetsing. *2.1 Impactanalyse en plan van aanpak nodig* Voor deze nieuwe wet wordt een impactanalyse uitgevoerd en een plan van aanpak opgesteld, zodat het bestuur kan besluiten over de benodigde maatregelen en middelen. Op diverse onderdelen zijn al voorbereidingen getroffen, rekening houdend met de nieuwe wet. Hierbij gaat het bijvoorbeeld om de systemen die gebruikt worden ivm de verhuizing (hier wordt een 0-meting op uitgevoerd). Daarnaast wordt de CbW betrokken (via extern advies) bij de aanbesteding van de kantoorautomatisering en het zaaksysteem.
Bijlagen	
Communicatie persbericht	-