provincie Zuid-Holland

GS brief aan Provinciale Staten

Provinciehuis
Postbus 90602
2509 LP Den Haag
T 070 - 441 66 11
www.zuid-holland.nl/contact

Datum
16 december 2025

Ons kenmerk
PZH-2025-884156749
DOS-2025-0002938

Bijlagen
1

Aan Provinciale Staten

Onderwerp:
Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027

Geachte Statenleden,

Op 16 april 2025 is in de Commissie Bestuur, Maatschappij en Middelen (BMM) het vorige informatieveiligheidsplan besproken. Tijdens deze bespreking is, mede op basis van nieuwe inzichten, de komst van een nieuwe Chief Information Security Officer (CISO) en verscherping van relevante wetgeving (onder andere de Europese Netwerk- en Informatiebeveiligingsrichtlijn 2 (NIS2)), toegezegd dat het plan geactualiseerd zou worden en opnieuw aan u zou worden voorgelegd.

Met deze brief wordt u aangeboden het geactualiseerde Plan van aanpak Weerbaarheid en Informatieveiligheidsplan PZH 2025-2027. Dit plan is opgesteld in nauwe samenwerking met het Informatieveiligheidsteam (IV-team), interne disciplines en externe partners, en sluit aan bij het coalitieakkoord 2023–2027.

Kernpunten van het geactualiseerde plan:

- **Verscherpte wet- en regelgeving:** Door de implementatie van de NIS2-richtlijn, Cyberbeveiligingswet (CBW), de Baseline Informatiebeveiliging Overheid 2 (BIO2) en externe audits zijn de eisen aan informatieveiligheid voor de provincie aanzienlijk aangescherpt. Informatieveiligheid is nu een organisatiebrede verantwoordelijkheid, die alle domeinen, processen en medewerkers raakt.
- **Programmatische en adaptieve aanpak:** Het plan werkt cyclisch en adaptief, met structurele borging van capaciteit en middelen. Nieuwe risico’s en wettelijke verplichtingen kunnen aanvullende inzet en middelen vragen, die via reguliere begrotingscycli worden geadresseerd. Dit zal gebeuren als integraal onderdeel van beleidsambities en -doelen en de bijbehorende opgavebudgetten.
- **Bestuurlijke prioritering:** Actieve steun vanuit Gedeputeerde Staten (GS), het Directieteam (DT), directeuren en het Ambtelijk Opdrachtgeversoverleg (AOG) is noodzakelijk voor succesvolle implementatie. Zonder concernbrede inzet is succesvolle implementatie van NIS2 en een organisatiebreed Information Security Management System (ISMS) niet haalbaar.
- **Incident- en continuïteitsmanagement:** Het plan versterkt crisisorganisatie, incidentrespons en herstelvermogen om de continuïteit van kritieke processen te waarborgen en te voldoen aan wettelijke eisen (NIS2, BIO).
- **Samenwerking:** Er is intensieve samenwerking met andere provincies en landelijke partners zoals het Nationaal Cyber Security Centrum (NCSC), het Ministerie van Binnenlandse Zaken

en Koninkrijksrelaties (MinBZK) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Ketenpartners en leveranciers worden actief betrokken bij risicobeheer en implementatie.
- **Communicatie en bewustwording:** Interne communicatie, educatie en bewustwording zijn structureel onderdeel van het plan. Externe/publicitaire aandacht is mogelijk bij majeure incidenten of bij het behalen van certificeringen.
- **Privacy en compliance:** Het plan houdt rekening met de Algemene Verordening Gegevensbescherming (AVG) en de BIO2.

Classificatie: Ten opzichte van het vorige plan is de classificatie aangepast van ‘geheim’ naar ‘openbaar’. Dit is mogelijk doordat het geactualiseerde plan minder operationele details bevat en meer gericht is op beleidsmatige en programmatische kaders. Hierdoor kan het plan breder gedeeld worden, terwijl gevoelige informatie nog steeds adequaat beschermd blijft.

Het plan wordt u ter informatie aangeboden. Indien gewenst kan het onderwerp besproken worden in een volgende commissievergadering.

Hoogachtend,

Gedeputeerde Staten van Zuid-Holland,

secretaris,	voorzitter,
drs. M.J.A. van Bijnen MBA	mr. A.W. Kolff

Bijlage:
Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027