provincie Zuid-Holland

GS-Voorstel
Besluitnummer
PZH-2025-884156749
DOS-2025-0002938

Status	Datum vergadering Gedeputeerde Staten	Eindtermijn
Openbaar	16 december 2025	n.v.t.

Onderwerp
Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027

Advies
1. Vast te stellen Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027
2. Vast te stellen Brief aan Provinciale Staten betreffende: Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027
3. Vast te stellen Publiekssamenvatting: Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027

Besluit GS
Vastgesteld met een machtiging voor de portefeuillehouder om:
- In de publiekssamenvatting in de 1e zin ‘provincie Zuid-Holland’ te wijzigen in ‘provinciale organisatie’;
- In het GS-voorstel bij het financieel kader te verduidelijken dat de €1,5 miljoen reeds gedekt is.

Bijlagen
- Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027 v1.66
- GS brief aan Provinciale Staten betreffende: Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027

1 Toelichting voor het College

De provincie Zuid-Holland staat voor de opgave om informatieveiligheid en weerbaarheid structureel te versterken. Informatieveiligheid is een strategische investering die onze weerbaarheid vergroot en als katalysator werkt voor professionalisering en toekomstbestendigheid. Het plan beschrijft een programmatische, cyclische en adaptieve aanpak in zes deels parallelle fasen, met bijzondere aandacht voor vitale infrastructuur, kritieke processen en essentiële informatiesystemen. Incidentmanagement, crisismanagement en bedrijfscontinuïteits- en herstelplannen (BCP/DRP) zijn expliciet als kernprocessen opgenomen.

Het plan sluit aan op aangescherpte wet- en regelgeving (zoals NIS2, CBW, BIO2) en de ambitie van de provincie om veilige, betrouwbare en toekomstbestendige dienstverlening te bieden aan inwoners, bedrijven en partners. Nieuwe risico's en wettelijke verplichtingen worden gekoppeld aan domeinen en opgaven; budgettaire verantwoordelijkheid ligt bij de betreffende opgave. Het plan vraagt om actieve betrokkenheid van bestuur, directieteam, domeindirecteuren, ambtelijk opdrachtgevers en medewerkers, en versterkt de samenwerking met ketenpartners en landelijke organisaties.

De succesvolle uitvoering van het plan vraagt om voortdurende aandacht voor risico's én succesfactoren. Belangrijke risico's zijn onder meer: onvoldoende urgentie of prioriteit, beperkte beschikbaarheid van middelen en capaciteit, weerstand tegen verandering en het onderschatten van nieuwe dreigingen. Succesfactoren zijn bestuurlijke prioritering, heldere communicatie, betrokkenheid van proceseigenaren en medewerkers, en een cultuur waarin informatieveiligheid vanzelfsprekend is. Door te sturen op deze factoren en risico's tijdig te signaleren en te beheersen, vergroot de provincie de kans op een effectieve en duurzame versterking van informatieveiligheid en weerbaarheid.

De uitvoering van het plan is afhankelijk van voldoende capaciteit en middelen. De basisfinanciering voor de kernactiviteiten van informatieveiligheid is geregeld via de Najaarsnota 2024. Aanvullende middelen die nodig zijn voor het afdekken van nieuwe risico's of wettelijke verplichtingen dienen via de reguliere begrotingscycli van de betreffende opgave te worden aangevraagd en verantwoord.

Financieel en fiscaal kader

Totaalbedrag excl. BTW	: € 1.500.000,- (per jaar / onderdeel van de meerjarenbegroting PZH, reeds gedekt)
Programma	: Ambitie 8.1.1 Een duurzame informatievoorziening en digitalisering
Financiële risico's	: er zijn geen financiële risico's

Juridisch kader

- Het IV-plan heeft geen juridische gevolgen in negatieve zin, mits de maatregelen uit het plan worden uitgevoerd. In positieve zin draagt het plan eraan bij dat de provincie Zuid-Holland beter voldoet aan relevante wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), de Wet open overheid (Woo), de Archiefwet, de Baseline Informatiebeveiliging Overheid (BIO/BIO2) en de Cyberbeveiligingswet (CBW, implementatie van de Europese Netwerk- en Informatiebeveiligingsrichtlijn 2 (NIS2)). Door uitvoering van het plan kan de provincie aantoonbaar voldoen aan de strengere eisen op het gebied van informatieveiligheid, incidentmelding, risicomanagement, ketenbeveiliging en continuïteitsplanning.

Niet of onvoldoende voldoen aan deze verplichtingen kan leiden tot toezichtmaatregelen of bestuurlijke boetes.

2 Voorafgaande besluitvorming

Het vorige informatieveiligheidsplan (2024) is op 16 april 2025 besproken in de commissie BMM en met Provinciale Staten. Tijdens die bespreking is aangegeven dat, mede op basis van nieuwe inzichten, de komst van een nieuwe CISO en aangescherpte wetgeving (waaronder NIS2), het plan zou worden aangepast. Dit voorliggende plan vervangt daarmee het plan uit 2024 en sluit aan bij het coalitieakkoord 2023-2027.

3 Proces

Het programmaplan Informatieveiligheid 2025-2027 is tot stand gekomen in nauwe samenwerking met de relevante onderdelen van de ambtelijke organisatie. Het plan is breed afgestemd binnen de organisatie en besproken in de daarvoor aangewezen gremia, waaronder het directieteam, domeindirecteuren en de ambtelijk opdrachtgevers.
Specifiek is het IV-plan besproken in de Regiegroep Digitale Transformatie (directeurenoverleg), waarbij de ontvangen feedback is verwerkt in de definitieve versie. Vervolgens is het plan ter vaststelling voorgelegd aan het Directieteam (DT). Na vaststelling door Gedeputeerde Staten wordt het programmaplan ter informatie aangeboden aan Provinciale Staten. Hiermee wordt geborgd dat zowel bestuurlijk als ambtelijk draagvlak aanwezig is voor de uitvoering van het plan.

4 Participatie en rolneming

Om het programma Informatieveiligheid succesvol te laten zijn, is een brede inbedding in de gehele organisatie noodzakelijk. De Regiegroep Digitale Transformatie (directeurenoverleg), waarin directeuren vanuit verschillende domeinen, Mens & Organisatie en Concerncontrol zijn vertegenwoordigd, speelt hierin een centrale rol.

Deze brede participatie waarborgt dat informatieveiligheid niet alleen een verantwoordelijkheid is van het IV-team, maar gedragen wordt door de hele organisatie. Zowel het Directieteam, directeuren, ambtelijk opdrachtgevers (AOG's), ambtelijk ondersteuners (AON's) als medewerkers zijn actief betrokken bij de uitvoering en borging van de maatregelen. Dit zorgt voor een integrale aanpak, waarbij informatieveiligheid structureel wordt verankerd in beleid, processen en cultuur van de Provincie Zuid-Holland.

5 Communicatiestrategie

Voor de communicatie over het programma Informatieveiligheid wordt gebruikgemaakt van zowel bestaande als nieuwe communicatiemiddelen binnen de Provincie Zuid-Holland. De communicatie richt zich op het vergroten van het bewustzijn rondom informatieveiligheid en het stimuleren van zorgvuldig omgaan met data en informatie binnen de organisatie. Zo wordt onder andere de communicatiecampagne 'Zo doen we dat' ingezet om het programma onder de aandacht te brengen.

Naast de reguliere interne communicatiekanalen wordt in 2026 ingezet op gerichte bewustwordingscampagnes, zoals als onderdeel van de campagne Zo Doen We Dat de sessie "Hoe AI op een veilige manier te gebruiken" in januari 2026, en op interactieve werkvormen zoals crisis oefeningen. Deze activiteiten zijn bedoeld om bestaande processen te testen, de rolverdeling verder aan te scherpen en informatieveiligheid op een laagdrempelige en aansprekende manier onder de aandacht te brengen. Hiermee wordt het gewenste gedrag in de praktijk versterkt.

Door communicatie en participatie te combineren, wordt informatieveiligheid een vanzelfsprekend onderdeel van het dagelijks handelen binnen PZH.