Plan van aanpak Weerbaarheid en Informatieveiligheid PZH 2025-2027

Met focus op de vitale infrastructuur, kritieke processen en essentiële informatiesystemen van de provincie

INFORMATIEVEILIGHEID TEAM

Inhoud

Versie	Datum	Status	Rol
V1.66	9-Dec-2025	Eindversie	CISO

1. Samenvatting

Informatieveiligheid is een strategische investering die onze weerbaarheid vergroot en als katalysator werkt voor professionalisering en toekomstbestendigheid.

Dit plan bouwt voort op de stappen die de Provincie Zuid-Holland de afgelopen jaren heeft gezet op het gebied van informatieveiligheid. Binnen zowel de IT-afdeling als de operationele techniek (OT) zijn processen en systemen ingericht, waaronder een Information Security Management System (ISMS) en een Cyber Security Management Control (CSMC). Deze basis stelt de provincie in staat om digitale risico's te beheersen en de continuïteit van kritieke processen te waarborgen.

Tegelijkertijd nemen de complexiteit van de digitale omgeving, de maatschappelijke afhankelijkheid van digitale diensten en externe dreigingen in hoog tempo toe. Nieuwe wetgeving, zoals de Europese NIS2-richtlijn, stelt daarbij strengere eisen aan de provincie als essentiële entiteit. Dit vraagt om een verbreding en verdieping van onze aanpak: informatieveiligheid is niet uitsluitend een IT- of OT-vraagstuk, maar raakt alle domeinen, opdrachten, processen en medewerkers. Of het nu gaat om beleid, vergunningverlening, vitale infrastructuur, informatiesystemen, persoonsgegevens of samenwerking met ketenpartners: informatieveiligheid raakt alle domeinen.

Dit plan biedt een programmatische aanpak in zes fasen om informatieveiligheid en weerbaarheid organisatiebreed te versterken, met speciale aandacht voor vitale infrastructuur, kritieke processen en essentiële informatiesystemen. Naast de zes implementatiefasen lopen acht kernprocessen continu door. De aanpak omvat zowel strategische sturing, risicobeheersing, bewustwording, de implementatie van maatregelen als het structureel borgen en door ontwikkelen van informatieveiligheid binnen de reguliere bedrijfsvoering.

Het plan vraagt om actieve betrokkenheid van Gedeputeerde Staten (eindverantwoordelijk), het management (directieteam, domeindirecteuren en ambtelijk opdrachtgevers), opdrachtnemers, proceseigenaren en medewerkers. Informatieveiligheid is een organisatiebrede verantwoordelijkheid die alleen effectief kan worden geborgd als alle lagen binnen de organisatie hun rol pakken. Daarnaast is een goede samenwerking tussen disciplines en opdrachten zoals IT, OT, privacy, concernrisicomanagement en M&O hierbij van groot belang. Dit plan richt zich daarom ook op het verder versterken en structureren van die samenwerking, zodat informatieveiligheid integraal onderdeel wordt van zowel de sturing als de uitvoering van de organisatie.

Het plan sluit aan op de strategische doelen van Gedeputeerde Staten, zoals verankerd in het coalitieakkoord, en ondersteunt de ambitie om te komen tot veilige, betrouwbare en toekomstbestendige (digitale) dienstverlening aan inwoners, bedrijven en partners.

Dit plan vervangt het vorige (2024) en speelt in op aangescherpte wetgeving, de overgang van vrijblijvendheid naar verplichting en een bredere scope voor de hele organisatie. Het sluit aan bij strategische doelen en ondersteunt versnelde professionalisering en een veilige, betrouwbare en toekomstbestendige digitale dienstverlening.

2. Wetgeving

De provincie Zuid-Holland opereert binnen een uitgebreid wettelijk kader dat de basis vormt voor haar informatiebeveiligingsbeleid. Hierbij spelen onder andere de volgende regelgevingen en standaarden een cruciale rol:

- **NIS2-richtlijn en Cybersecuritywet (Cbw)**
  De Europese NIS2-richtlijn wordt in Nederland geïmplementeerd in de Cyberbeveiligingswet. Als essentiële entiteit is de provincie verplicht om adequate beveiligingsmaatregelen te treffen, incidenten te melden, en valt qua toezicht onder de Rijksinspectie Digitale Infrastructuur. De NIS2 richtlijn stelt hoge eisen aan bestuurlijke betrokkenheid, risicomanagement, ketenbeveiliging, en continuïteitsplannen.
- **Algemene Verordening Gegevensbescherming (AVG)**
  De bescherming van persoonsgegevens is wettelijk verplicht en vereist dat passende technische en organisatorische maatregelen worden genomen om de privacy van burgers te waarborgen.
- **Andere relevante wet- en regelgeving**
  Onder meer de Archiefwet en Wet open overheid (Woo) stellen aanvullende eisen aan het beheer, de beveiliging en beschikbaarheid van informatie.
- **Normenkaders en standaarden**
  De provincie volgt de Baseline Informatiebeveiliging Overheid (BIO), die gebaseerd is op de internationale ISO 27001-norm. De BIO wordt momenteel geactualiseerd naar BIO2, die de nieuwe eisen van NIS2 integreert, waaronder verplichtstelling voor de provincies, en daarmee het wettelijk toetsingskader voor de provincie wordt.
- **Europese ambities en aanvullende kaders**
  De informatiebeveiligingsopgave van de provincie staat niet op zichzelf, maar maakt deel uit van bredere Europese ambities zoals verwoord in het programma ‘Digital Decade 2030’, waarin digitale soevereiniteit, veilige digitale infrastructuren en interoperabiliteit tussen overheden centrale thema’s zijn. Binnen deze context groeit het aantal relevante wet- en regelgevingen op het gebied van digitale veiligheid en gegevensdeling. Denk hierbij aan de AI Act, die eisen stelt aan het veilig toepassen van kunstmatige intelligentie, en de aanstaande Cyber Resilience Act, die aanvullende verplichtingen introduceert voor de beveiliging van digitale producten en software. Ook op het gebied van datawetgeving neemt het belang van cyberbeveiliging toe. Wetgeving als de Data Governance Act en de Data Act stimuleren het delen van data binnen en tussen overheden, maar stellen tegelijk stevige eisen aan de beveiliging en controle over die data. Cyberbeveiliging vormt daarmee steeds vaker een harde randvoorwaarde voor digitale samenwerking, transparantie en innovatie binnen de overheid.

Impact voor de provincie

De aangescherpte wet- en regelgeving, zoals de NIS2-richtlijn, de Cyberbeveiligingswet en de geactualiseerde BIO2, heeft directe en ingrijpende gevolgen voor de Provincie Zuid-Holland. Als essentiële entiteit wordt van de provincie verwacht dat zij haar informatieveiligheid structureel en organisatiebreed op een hoger niveau brengt. Dit betekent dat niet alleen de IT-afdeling, maar alle domeinen, processen en medewerkers moeten voldoen aan strengere eisen op het gebied van risicomanagement, ketenbeveiliging, incidentmelding en continuïteitsplanning.

De impact is zichtbaar op meerdere vlakken:

- **Bestuurlijk:** Er is een grotere bestuurlijke verantwoordelijkheid en betrokkenheid vereist, met expliciete sturing en rapportage aan Gedeputeerde Staten.
- **Organisatorisch:** Informatieveiligheid wordt een integraal onderdeel van alle processen, met een verbreding van de scope naar de gehele organisatie en een nadruk op eigenaarschap en samenwerking.
- **Operationeel:** Medewerkers en proceseigenaren moeten zich bewust zijn van hun rol in informatieveiligheid, ondersteund door structurele training en gedragsverandering.
- **Technisch:** Er zijn investeringen nodig in tooling, monitoring en incidentmanagement om te voldoen aan de nieuwe normen en om audits en certificering mogelijk te maken.
- **Juridisch:** De provincie moet aantoonbaar voldoen aan de wettelijke verplichtingen, wat vraagt om continue toetsing, documentatie en aanpassing van beleid en procedures.

Kortom, de provincie staat voor de opgave om informatieveiligheid te verankeren als strategische randvoorwaarde voor haar dienstverlening en bedrijfsvoering. Dit vraagt om een programmatische, risicogestuurde aanpak en voldoende capaciteit en middelen om aan de huidige en toekomstige eisen te voldoen.

3. Uitgangspunten

De provincie Zuid-Holland ziet informatieveiligheid als een **blijvende strategische opgave**. De afhankelijkheid van digitale systemen groeit, net als de dreiging van cyberaanvallen en de relevantie van digitale autonomie. De verwevenheid van ketens, omgevingsdiensten, leveranciers en technologieën maakt dit vraagstuk extra urgent.

1. Informatieveiligheid als strategische randvoorwaarde

Informatieveiligheid is essentieel voor het behalen van de doelstellingen van PZH. Burgers en bedrijven moeten kunnen vertrouwen op de beschikbaarheid, betrouwbaarheid en integriteit van álle waardevolle onderdelen van de provincie. Dit omvat niet alleen informatie, maar ook kritieke processen, infrastructuur, fysieke assets zoals bruggen en sluizen, en andere voorzieningen waarop burgers en bedrijven vertrouwen. Daarom is structurele inbedding van informatieveiligheid in de hele organisatie nodig - inclusief cultuur, capaciteit en eigenaarschap.

2. Aanscherping wet- en regelgeving

Nieuwe wet- en regelgeving, zoals de Europose NIS2-richtlijn, die in Nederland geïmplementeerd wordt via de Cyberbeveiligingswet (Cbw) en de vernieuwde BIO, brengen hogere eisen met zich mee. PZH committeert zich aan:

- **BIO2** voor overheidsbrede basisnormen;
- **ISO 27001** als generieke norm voor informatiebeveiliging;
- **IEC 62443** voor operationele technologie (OT).

3. Risicogestuurde aanpak

Risicomanagement is het centrale sturingsinstrument. Het stelt PZH in staat om haar vitale infrastructuur, kritieke processen en essentiële informatiesystemen goed in kaart te hebben, prioriteiten te stellen, middelen effectief in te zetten en aantoonbaar te voldoen aan eisen. Deze aanpak is verankerd in het Information Security Management System (ISMS) en sluit aan op het cyclische Plan-Do-Check-Act (PDCA)-principe van continue verbetering.

4. Samenwerking als voorwaarde voor succes

Informatieveiligheid is een gedeelde verantwoordelijkheid. Het vraagt om actieve betrokkenheid van Gedeputeerde Staten (eindverantwoordelijk), en nauwe samenwerking tussen het management (directieteam, domeindirecteuren en ambtelijk opdrachtgevers), opdrachtnemers, proceseigenaren, medewerkers en externe partners zoals leveranciers en toezichthouders. Alleen via gezamenlijke inzet kunnen risico's tijdig worden herkend en beheerst.

5. Gedragsverandering als fundament

Veilig gedrag is essentieel. Medewerkers, externe inhuur en bestuurders moeten risico's herkennen en veiligheid vanzelfsprekend meenemen in hun handelen. Daarom wordt ingezet op structureel bewustzijn, herhaling en voorbeeldgedrag vanuit management. Gedragsverandering is geen bijzaak of iets eenmaligs, maar een structureel onderdeel van het informatieveiligheidsbeleid.

6. Informatieveiligheid als investering

Investeren in informatieveiligheid levert meer op dan minder incidenten, hogere betrouwbaarheid van systemen, lagere beheerkosten en beter risicobeheer. Het brengt een professionaliseringsslag tot stand: processen worden gestandaardiseerd, verantwoordelijkheden verankerd en medewerkers ontwikkelen de kennis en vaardigheden die nodig zijn voor een toekomstbestendige werkwijze. Door beveiliging structureel te integreren in processen ontstaat niet alleen een robuuste, maar ook een volwassen en professioneel georganiseerde provincie die klaar is voor nieuwe uitdagingen.

4. Huidige situatie

De afgelopen twee jaar heeft de organisatie aanzienlijke stappen gezet om de naleving van de BIO en ISO 27001 te verbeteren binnen zowel de IT- als OT-omgevingen. Dit is onder meer zichtbaar in de positieve ontwikkeling van het IT-beveiligingsniveau: een audit in november 2023 toont een stijging van 31% naar 74% binnen de onderzochte scope. Belangrijk hierbij is dat deze audit slechts een deel van de organisatie besloeg, waardoor bredere uitrol en toetsing noodzakelijk blijven. Op basis van de huidige resultaten bevindt de provincie zich qua volwassenheid tussen niveau 1 en 2. Voor structurele borging en externe certificeerbaarheid is verdere groei richting volwassenheidsniveau 3 vereist (zie voor volwassenheidsniveaus ook de volgende sectie “Gewenste situatie”).

In opdracht van het IPO (Meerjarenplan digitalisering, AAC digitalisering) is tevens een NIS2 impactanalyse uitgevoerd, die bevestigt dat de organisatie gemiddeld scoort. Cruciale aandachtspunten zijn het ontbreken van organisatiebrede risicoanalyses, een kloof tussen beleid en praktijk, gebrekkige toetsing van maatregelen en onvoldoende inzicht in leveranciersrisico’s. Deze bevindingen vragen om inzet van zowel het informatieveiligheid team als uitvoerende afdelingen, die capaciteit moeten inregelen en vrijmaken voor risicogestuurd werken en het borgen van informatieveiligheid.

De OT-omgeving, waarin bedrijfskritieke systemen zoals bruggen en sluizen worden beheerd, ondergaat een vergelijkbare transitie. Technologische integratie van IT en OT vergroot zowel de operationele mogelijkheden als de risico’s. Een GAP-analyse op basis van IEC 62443 toont aan dat verdere implementatie van beheersmaatregelen, risicomanagement en OT-specifieke awareness-programma’s noodzakelijk zijn om aan NIS2 te voldoen.

Het opzetten van een samenhangend Cyber Security Management Systeem (CSMS) is in volle gang.

De organisatie heeft ingezet op een geïntegreerd Information Security Management System (ISMS) dat via een cyclisch PDCA-model continu verbetert. Succes hiervan vereist actieve betrokkenheid en capaciteit op alle niveaus van de organisatie, en sluit aan bij de bredere ambitie voor gedragsverandering als fundament door middel van cultuurverandering en bewustwording. Verschillende projecten en programma’s ondersteunen deze ontwikkeling, waaronder Informatietransitie, Identity & Access Management (IAM), Managed Detection & Response (MDR), Educatie en Awareness programma en bewustwordingscampagnes.

Bestuurlijk is het onderwerp steviger verankerd door de recente oprichting van strategische en tactische overlegvormen, waarin onder andere de provincie secretaris, CISO en functionarissen van relevante wetgevingen en vertegenwoordigd zijn. Daarnaast werkt de organisatie intensief samen met andere provincies en landelijke partners zoals het NCSC en CIBO, wat bijdraagt aan kennisdeling en een eenduidige aanpak.

Kortom, terwijl belangrijke stappen zijn gezet, vraagt de toenemende complexiteit van regelgeving, digitalisering en samenhang tussen IT en OT om voortdurende aandacht en investering. Alleen zo kan de organisatie voldoen aan de actuele en toekomstige eisen op het gebied van informatieveiligheid en daarmee de risico’s voor de provinciale organisatie effectief beheersen.

5. Gewenste situatie

De Provincie Zuid-Holland zet zich in voor een gefaseerde implementatie van de Cyberbeveiligingswet (Cbw), met als doel de volledige operationele integratie uiterlijk eind 2027. Dit is onder voorbehoud van de formele vaststelling van de wet en de beschikbaarheid van voldoende middelen.

De prioriteiten in dit plan zijn bepaald op basis van de eisen uit de Cyberbeveiligingswet (NIS2), bevindingen uit interne en externe audits, gap-analyses, risicomanagement het bereiken van volwassen- heidsniveau 3 (proactieve beheersing). Dit niveau is noodzakelijk om daadwerkelijk ISO 27001-gecertificeerd te kunnen worden

De aanpak is gebaseerd op 6 deels parallelle fasen (zie hoofdstuk 6), startend met het stabiliseren van de huidige basis om zich te ontwikkelen naar een organisatiebrede uitrol met versterking van governance, tooling, cultuur en continuïteit. In iedere fase zijn rollen en verantwoordelijkheden vastgelegd, waarbij het informatieveiligheidsteam verantwoordelijk is voor regie, coördinatie en monitoring, en de domeinen voor uitvoering binnen hun eigen processen.

De kernambities voor 2025–2027 zijn:

- **Risicogestuurd Werken en Structurele Borging:** Organisatiebreed informatiebeveiligingsrisico's systematisch identificeren, analyseren en beheersen. Verankering van risicomanagement over de hele levenscyclus, van ontstaan, bestaan tot vergaan, in processen, eigenaarschap, rapportage , management sturing en besluitvorming.
- **Aanschaf en implementatie van ISMS-tooling:** ISMS-tooling implementeren voor effectieve bewaking, uitvoering en rapportage en het faciliteren van audits en certificering.
- **Incidentpreventie en -respons:** Preventieve maatregelen versterken en incidentmanagementproces verscherpen voor naleving van (inter)nationale regelgeving zoals NIS2 en verhogen de veerkracht tegen cyberdreigingen.
- **Bewustzijn en Opleiding:** Bewustzijn en kennis van medewerkers structureel versterken via verplichte trainingen.
- **Certificering:** Streven naar ISO 27001-certificering als bewijs van een gedegen beveiligingskader.

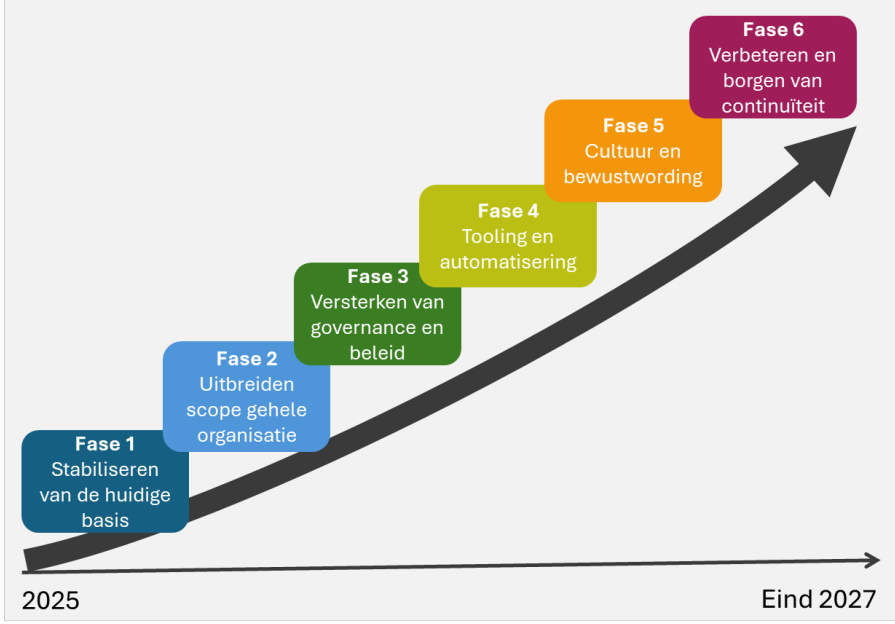
Een robuust governancemodel borgt de samenwerking tussen Gedeputeerde Staten (eindverantwoordelijk), het management (directieteam, domeindirecteuren en ambtelijk opdrachtgevers), het IV-team en de uitvoerende afdelingen. Tevens wordt actief samengewerkt met ketenpartners en andere overheden om gezamenlijke risico's effectief te beheersen.

Het behalen van deze ambities is afhankelijk van voldoende budget en inzet van gekwalificeerd personeel. Voortgang en resultaten worden systematisch gemonitord en periodiek gerapporteerd aan Gedeputeerde Staten, wat transparantie en sturing waarborgt.

De aanpak is ingebed in een continu verbeterproces volgens de PDCA-cyclus (Plan–Do–Check–Act), waarmee de Provincie Zuid-Holland haar digitale weerbaarheid toekomstbestendig maakt en houdt.

6. Plan van aanpak

Het plan van aanpak bestaat uit zes fasen. Deze fasen hebben een logische volgorde, van opbouw binnen het Informatie-veiligheidsteam naar organisatiebreed, en van structuur naar borging, maar worden in de praktijk grotendeels parallel uitgevoerd. Dit betekent dat we niet wachten tot een fase volledig is afgerond voordat we aan de volgende beginnen. Waar mogelijk pakken we activiteiten gelijktijdig op om snelheid en samenhang te bevorderen.



Naast de zes implementatiefasen lopen acht kernprocessen continu door. Deze processen kunnen onderdeel zijn van een van de fasen maar worden daarnaast ook apart benoemd en aangepakt.

Fase 1 – Stabiliseren van de huidige basis
Focus op het op orde houden en verfijnen van bestaande informatieveiligheidsprocessen, zoals incidentmanagement, risicoanalyses en audits. Ook samenwerking binnen bestaande interprovinciale gremia en met ketenpartners valt hieronder. Dit is grotendeels het “eigen terrein” van het IV-team en vraagt om continuïteit en optimalisatie. Te nemen stappen zijn:

- Continueren en borgen van lopende processen
- Incidentmanagement aanscherpen, onder andere door snellere detectie (via MDR voor IT), forensics retainer, crisis oefeningen
- Risico’s monitoren binnen bestaande scope
- Samenwerkingsverbanden onderhouden
- Ondersteunen van audits en penetratietests

Fase 2 – Uitbreiden van de scope naar organisatiebreed niveau
In deze fase verschuift het zwaartepunt naar de hele organisatie. Domeinen brengen, waar dat nog niet gebeurd is, hun risico’s, applicaties, processen en leveranciers in kaart. Het IV-team faciliteert, coördineert en stelt kaders, maar heeft minder directe regie. Heldere afspraken, governance en eigenaarschap in de lijn zijn hier cruciaal. Voor nieuwe geïdentificeerde risico’s worden nieuwe activiteiten opgezet worden. Te nemen stappen zijn:

- In kaart brengen en risicoanalyse van alle domeinen en processen
- Betrekken van nieuwe scope en stakeholders
- Inventariseren en beoordelen van risico’s m.b.t. leveranciers
- Valideren van vitale infrastructuur, kritieke processen en essentiële informatiesystemen in de organisatie brede context (nog niet in de huidige scope)
- Verbeteren kernprocessen zoals Business Continuïteit Plan en aansluiten op de vitale infrastructuur, kritieke processen en essentiële informatiesystemen
- Domein uitvoering OT- opvolging uitkomsten GAP analyse
- Domein uitvoering opzetten MDR dienst voor OT

Fase 3 – Versterken van governance en beleid
Deze fase richt zich op het verder vastleggen van

verantwoordelijkheden, mandaten en rapportagelijnen, binnen het kader van informatieveiligheid. Ook formatieplanning, capaciteitstoewijzing en de positionering van het IV-team maken hier deel van uit. Governance vormt de brug tussen centrale sturing en decentrale uitvoering. Te nemen stappen zijn:

- Rollen, verantwoordelijkheden en taken formaliseren op alle niveaus (operationeel, tactisch, strategisch)
- Actualiseren en valideren van beleid en procedures
- Rapportagestructuren opzetten voor risicobeheer en voortgangsmonitoring, management sturing

Fase 4 – Tooling en automatisering
Selectie en implementatie van ISMS-tooling en ondersteunende systemen voor registratie, monitoring en rapportage. De functionele inrichting ligt grotendeels bij het IV-team, maar succesvolle toepassing vraagt om betrokkenheid van gebruikers, procesverantwoordelijken en ICT-beheer. Te nemen stappen zijn:

- Selectie en implementatie van ISMS-tooling
- Integratie van tooling met privacy- en OT-beveiliging
- Onderzoek naar consolidatie van beheer- en controle-instrumenten (ISMS, CSMC, privacy verwerkingregisters)

Fase 5 – Cultuur en bewustwording
Draagt bij aan duurzame gedragsverandering door trainingen, communicatie en leiderschap. Het IV-team ontwikkelt formats en ondersteunt campagnes, maar blijvende impact vereist actieve betrokkenheid van M&O, communicatie en het management. Te nemen stappen zijn:

- Doorontwikkelen van informatieveiligheid en privacy educatie en bewustzijn-programma's
- Risicobewustzijn en informatieveilig gedrag stimuleren binnen de gehele organisatie
- Verankeren van informatieveiligheid in M&O processen zoals onboardingprocessen

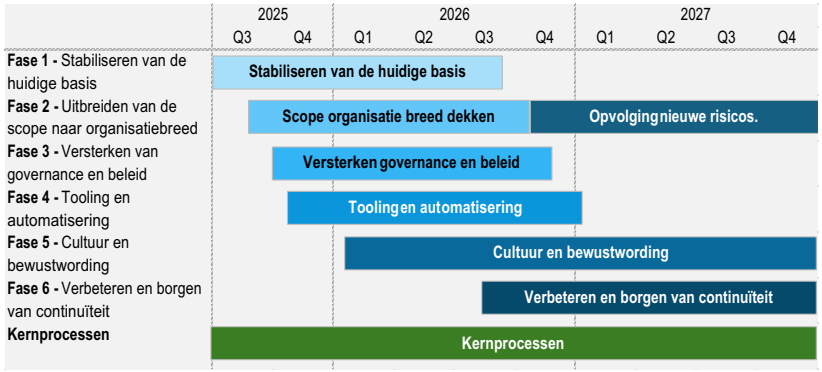
Fase 6 – Verbeteren en borgen van continuïteit
Alle processen worden ondergebracht in een structurele PDCA-cyclus. Resultaten van audits en monitoring worden systematisch opgevolgd. Voorbereiding op certificering (zoals ISO 27001) en blijvende weerbaarheid zijn hierin opgenomen. Dit is een gezamenlijke verantwoordelijkheid van IV en de hele organisatie. Te nemen stappen:

- Uitvoeren van periodieke audits en penetratietesten
- Structureel oplossen van auditbevindingen
- Bereiken en onderhouden volwassenheidsniveau 3 voor het ISMS
- ISO27001 certificatie

Parallel aan de zes fasen vindt een doorlopende verbetering van kernprocessen plaats - valideren, herinrichten en aanscherpen:

- Risicomanagement
- Security Incident management
- BCP/DRP en crisismanagement
- Processen rondom Managed Detection Response (MDR) / inclusief incident response en forensics retainer
- Inkoopproces en contract management
- Projectmanagement
- M&O-processen
- Leveranciers risico management

Planning:



De verdere uitwerking en sturing van deze planning vindt plaats in een programmaplan.

7. Risico's, Succesfactoren en Kritieke Afhankelijkheden

De succesvolle invoering van informatieveiligheid binnen PZH vraagt expliciet om management betrokkenheid en concernbrede aansturing.

Kritieke Afhankelijkheden

1. **Bestuurlijke prioritering**
   Dit is de meest bepalende factor voor succes of falen van het programma. Hierbij is actieve steun vanuit GS, DT en AOGs onontbeerlijk.
2. **Toereikende middelen**
   - Voor het IV-team: voldoende budget en gekwalificeerde medewerkers.
   - Voor de domeinen: zij zijn uitvoerend verantwoordelijk voor te treffen maatregelen.
3. **Organisatiecultuur en acceptatie**
   Informatieveiligheid vraagt bewustwording, gedragsverandering en voorbeeldgedrag op alle niveaus. Dit vraagt actieve communicatie, educatie en betrokkenheid.

Succesfactoren

- **Bestuurlijke prioritering** (opnieuw): bepalend voor legitimiteit, middelen én cultuurvorming.
- **Structurele congruente communicatie**: één lijn in boodschappen vanuit directie, programma's en beleid.
- **Procesverantwoordelijkheid**: betrokkenheid van proceseigenaren bij risico-inventarisatie en maatregeluitvoering.
- **Verbonden aan/Koppeling aan bredere opgaven**: Denk aan informatietransitie en continuïteit van primaire processen.
- **Continue verbetering**: Het ISMS werkt cyclisch (PDCA) en vereist voortdurende bijsturing.

Risico's die aandacht vragen

Risico	Bestuurlijk belang
Gebrek aan urgentie	Kan leiden tot verlies aan prioriteit, middelen en tempo.
Onvoldoende middelen	Bedreigt uitvoerbaarheid op meerdere niveaus.
Weerstand tegen verandering	Vraagt heldere uitleg, communicatie en voorbeeldgedrag.
Verkeerde of onvolledige risicobeoordeling	Leidt tot suboptimale of ontbrekende maatregelen.
Onvoldoende maatregelen	Reputatieschade en mogelijke boete.

Risicobeheersing en sturing

Om bovenstaande risico's te beheersen is er voorzien in:

- **Continue sturing door opdrachtgever(s)** op resultaten, prioriteiten en afhankelijkheden;
- **Frequente communicatie** over voortgang en dilemma's (richting DT, GS, AOG);
- **Inrichting van risicorapportages** op operationeel, tactisch én strategisch niveau;
- **Budgetbewaking en afstemming met interne en ook externe stakeholders**.

De onderstaande tabel laat zien welke onderdelen onder directe verantwoordelijkheid van het IV-team vallen en waar afhankelijkheid bestaat van domeinen of andere organisatieonderdelen. Goede samenwerking is hierbij cruciaal, omdat informatieveiligheid alleen effectief kan worden geborgd als alle betrokken partijen hun rol nemen. De genoemde voorbeelden zijn illustratief en niet uitputtend.

Fase	**Wat valt onder verantwoordelijkheid van het IV-team?**	**Wat valt onder de verantwoordelijkheid van de domeinen ?**
1. Stabiliseren huidige basis	- Incidentmanagement coördineren - Uitvoering audits en toetsen - Beheer risicoregisters - Interne afstemming en overleg binnen IV-gremia	- Operationele uitvoering door domeinen - Incidentmelding en eerste lijnsafhandeling bij teams buiten IV - Ondersteuning door ICT en OT-teams
2. Opschalen naar organisatiebreed niveau	- Initiëren en faciliteren risicobeoordelingen - Coördineren van organisatiebrede risico inventarisaties - Adviseren bij procesanalyses	- Uitvoeren risicoanalyses per domein - Invoeren maatregelen en aanpassingen in eigen processen - Verantwoordelijkheid van domein “eigenaren” voor eigen scope
3. Governance en beleid versterken	- Ontwikkelen en actualiseren van beleid en richtlijnen - Organiseren governance structuren (SIO, TIO, IV-team) - Rapportage inrichting en consolidatie	- Toepassing van beleid door domeinen - Verantwoordelijkheid van management en bestuur - Commitment van lijnmanagement voor naleving
4. Tooling en automatisering implementeren	- Selectie en beheer ISMS-tooling - Integratie van tooling binnen IV-processen - Training en ondersteuning toolgebruik	- Implementatie en gebruik tooling in domeinen - ICT ondersteuning voor integratie - Gebruikersacceptatie en feedback vanuit domeinen
5. Cultuur en bewustwording versterken	- Ontwikkelen educatie- en bewustzijn programma’s - Coördinatie inhoud verplichte IV en privacy trainingen - Monitoren bewustwordingseffecten	- Actieve deelname medewerkers - M&O rol in cultuurverandering en opleiding - Leidinggevenden stimuleren gedragsverandering
6. Verbeteren en borgen continuïteit	- Organiseren onafhankelijke audits - Analyseren auditresultaten en opvolgen bevindingen - Continu monitoren van ISMS-prestaties en PDCA cyclus	- Uitvoeren verbetervoorstellen door domeinen - Verankering in reguliere bedrijfsprocessen - Management review en besluitvorming

8. Capaciteit en Middelen

De implementatie van informatieveiligheid maatregelen en het versterken van informatieveiligheid binnen de Provincie Zuid-Holland om te voldoen aan de verscherpte wetgeving (NIS2, CBW, BIO2) staat of valt met voldoende gekwalificeerde medewerkers en middelen. Zowel op concernniveau als binnen het IV-team is sprake van knelpunten.

Menselijke Capaciteit – Kritieke randvoorwaarde

IV-team

- Het IV-team heeft momenteel lopende vacatures.
- Focus ligt noodgedwongen op de grootste risico's; structurele taken en nieuwe NIS2-verplichtingen kunnen niet volledig opgepakt worden.
- Complexiteit van de taken is toegenomen en de noodzakelijke uitbreiding van de scope naar de gehele organisatie vragen om uitbreiding van capaciteit.
- Een formatieplan is reeds voorgelegd aan M&O voor uitbreiding en herwaardering. De formatie wordt jaarlijks geëvalueerd.

Brede organisatie

- Ook buiten het IV-team ontstaan nieuwe taken door NIS2:
  - Bij beheerafdelingen (infra, applicaties, servicemanagement): door MDR-implementatie, penetratietests, risicoanalyses, etc.
  - Bij M&O: op gebieden zoals toegangsbeheer, onboarding/offboarding, performancebeleid en awareness-educatie.
- Structurele werkdruk in de uitvoering belemmert de realisatie van informatieveiligheidsdoelen.

Bestuurlijke implicatie: zonder inzet op formatie en concernbrede capaciteit is succesvolle implementatie van NIS2 en een concernbreed ISMS niet haalbaar.

Middelen – Financiële dekking en toekomstige noodzaak

- De financiering voor de kernactiviteiten van informatieveiligheid is toegekend via de Najaarsnota 2024 en is op voorhand voldoende.
- De afdelingen OT en IT beschikken over eigen plannen en budgetten die samenhangen met informatieveiligheidsdoelstellingen.
- Nieuwe risico's en wettelijke verplichtingen worden gekoppeld aan een domein/opgave.
- Budgettaire verantwoordelijkheid ligt bij die opgave.
- Het plan heeft in deze context ook als doel om opgaven bewust te maken van deze rol.

Tabel 1: Budget IV Informatieveiligheid (*1000)

Activiteit	Fase	2025	2026	2027	
Incident- en crisis (oefenen en training)	1	75	75	75	KeA
Security incident forensics retainer dienst	1	-	50	50	KeA
OT- opvolging GAP analyse	2	200	200	200	KeA
MDR voor de OT omgeving	2	100	350	350	KeA
ISMS/GRC-tooling	4	50	50	50	KeA
E-learning IV en Privacy	5	50	50	50	KeA
Audit naar BIO2 en ISO 27001	6	-	50	50	KeA
Penetratie testen en advies diensten	1, 6	90	90	90	KeA
Licenties, hw/sw, overige diensten	Alle	365	365	365	IWS
Programma manager	Alle	40	300	300	KeA
Vrije ruimte	Alle	30	-10	-10	-
Totaal		1000	1570	1570	
Budget		**1000**	**1570**		

KeA = Kaders en Advies

IWS = Infrastructuur Werplek Support

Bestuurlijke implicatie: informatieveiligheid vraagt om structurele borging en wendbaarheid

Dit informatieveiligheidsplan vormt een belangrijke stap in de versterking van onze veiligheid en weerbaarheid. De opgenomen activiteiten en bijbehorende middelen dekken de basis voor de komende jaren. Tegelijkertijd is het van belang te onderstrepen dat informatieveiligheid geen eenmalige inspanning is, maar een doorlopend programma dat zich voortdurend ontwikkelt.

Binnen dit risico gebaseerde programma worden risico's en kwetsbaarheden actief geïdentificeerd, geanalyseerd en geadresseerd. Dit betekent dat nieuwe inzichten, bijvoorbeeld uit gap assessments, audits, incidenten, of impact door veranderende wet- en regelgeving, kunnen leiden tot aanvullende maatregelen.

9. Definities

AVG - Europese wetgeving voor bescherming van persoonsgegevens.
BCP - Plan voor het waarborgen van kritieke processen bij crises.
BIO - Baseline Informatiebeveiliging Overheid; gebaseerd op ISO 27001.
BIO2 - Geactualiseerde versie van de BIO.
CBW - Cyberbeveiligingswet, Nederlandse implementatie van NIS2.
CISO - Chief Information Security Officer, verantwoordelijk voor informatieveiligheid.
CSMS - Cybersecurity Management System voor OT-omgevingen.
DRP - Plan voor herstel van IT-systemen na incidenten.
GRC - Governance, Risk & Compliance.
IAM - Identity & Access Management: regelt wie wanneer toegang heeft tot welke systemen.
IEC 62443 – Norm voor beveiliging van industriële systemen (zoals bruggen en sluizen).
ISMS - Information Security Management System, structuur voor informatiebeveiliging.
IPO - Interprovinciaal Overleg.
ISO - Information Security Officer; ondersteunt de CISO.
ISO 27001 - Internationale standaard voor ISMS.
IT/ICT - Informatie- en communicatietechnologie (zoals netwerken en systemen).
IV-team – Informatieveiligheid team of CISO team
MDR - Managed Detection & Response: dienst voor vroegtijdige detectie van cyberdreigingen.
M&O – Mens en Organisatie
NIS2 – Europese richtlijn voor cybersecurity, vertaald naar o.a. CBW en BIO2.
OT - Operationele techniek; systemen voor aansturing van fysieke processen.
PDCA - Plan-Do-Check-Act cyclus; basis voor continue verbetering van ISMS.
Woo - Wet open overheid; verplicht actieve openbaarheid van overheidsinformatie.

10. Bronnenlijst

- Jaarplan CIBO 2025
- Jaarplan OT - Themaplan Cyber Security 2025-2029
- Audit rapportage IT November 2023
- NCSC Op weg naar een cyberveilige NAVO-top - mei 2025
- NCTV actueel Dreigingsbeeld Terrorisme Nederland – december 2024
- Coalitieakkoord Provincie Zuid Holland 2023-2027