Informatieveiligheidsbeleid 2023 - 2025

Vastgesteld in het GS d.d. 10-01-2023

Afdeling Informatisering en Automatisering
Provincie Zuid-Holland
Januari 2023

Inhoudsopgave

1 Inleiding

1.1 Inleiding

Voor de provinciale organisatie is digitalisering een essentiële randvoorwaarde voor het goed functioneren van maatschappelijke processen en het ontwikkelen van de beleidsterreinen van provincie. De provincie heeft daarom koers gezet naar een transparantie overheid waarbij informatieveiligheid en privacy wordt geborgd. Informatieveiligheid is tegelijkertijd meer dan techniek alleen. Bewustwording en sturing op informatieveiligheid worden steeds belangrijker: het gaat om *business*, *bytes* en *behavior*.

Het motto "voorkomen is beter dan genezen" gaat voor informatieveiligheid zeker op. Provincie Zuid-Holland wil de informatieveiligheid verbeteren, waarbij wordt gericht op het op orde brengen en houden van de informatieveiligheid. Ook het bieden van een veilige digitale dienstverlening aan "klanten" van de provincie hoort daarbij.

1.2 Doelstelling

Het doel van het Informatieveiligheidsbeleid is het helpen waarborgen van de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de bedrijfsprocessen zodat PZH zijn taken optimaal kan uitoefenen. In dit geactualiseerde informatieveiligheidsbeleid wordt de governance en sturing versterkt. Het Beleid Informatieveiligheid zoals vastgesteld in juli 2014 komt hiermee te vervallen.

1.3 Reikwijdte

Het hier vastgelegde beleid geldt voor alle organisatieonderdelen van PZH waarvoor de Gedeputeerde Staten verantwoordelijk voor zijn. Het betreft de provinciale organisatie, bedrijfsprocessen, ICT- en OT en gebouwen van de provincie.

1.4 Geldigheid en evaluatie

Het informatieveiligheidsbeleid van de provincie wordt ten minste één keer per drie jaar geëvalueerd en zo nodig bijgesteld.

1.5 Leeswijzer

In hoofdstuk 2 wordt het onderwerp informatieveiligheid toegelicht. Hoofdstuk 3 gaat over de missie, visie, uitgangspunten en organisatie van de informatieveiligheid bij PZH. In hoofdstuk 4 wordt het ISMS en de uitgangspunten betreffende risicomanagement besproken.

2 Informatieveiligheid

2.1 Wat is informatieveiligheid?

De provincie Zuid-Holland is in toenemende mate afhankelijk van informatie die is opgeslagen in informatiesystemen en van informatiesystemen voor de aansturing van kunstwerken. Deze afhankelijkheid brengt nieuwe kwetsbaarheden en risico's met zich mee, die met passende maatregelen beperkt dienen te worden. De steeds groter wordende afhankelijkheid van de informatiesystemen leidt bijna automatisch tot allerlei veiligheidsvraagstukken die de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van deze informatiesystemen raken.

Informatieveiligheid[1] is het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen voor de bescherming van bedrijfsprocessen en belangen van de provincie op basis van risicomanagement. Maatregelen moeten gericht zijn op het garanderen van betrouwbaarheid van de informatievoorziening op een niveau dat past bij de behoefte vanuit de primaire provinciale organisatie. Het beleid en de uitvoering van informatiebeveiliging is een samenspel van bestuur, management, cultuur, processen en techniek.

Incidenten en inbreuken in de taakuitvoering van de provincie kunnen leiden tot maatschappelijke schade, financiële nadelen en imagoschade. Daarom is systematische aandacht aan de beveiliging van de informatievoorziening een vereiste, waarbij de nadruk steeds meer komt te liggen op het handelen bij en na een incident.

Binnen het vakgebied informatieveiligheid wordt onderscheid gemaakt in drie aspecten van betrouwbaarheid van de informatievoorziening: beschikbaarheid, integriteit en vertrouwelijkheid:

- **Beschikbaarheid:** Beschikbaarheid is de mate waarin informatie beschikbaar is voor de gebruiker en/of het systeem in bedrijf is op het moment dat de organisatie deze nodig heeft.
- **Integriteit:** Integriteit is de mate waarin de informatie actueel en zonder fouten is. Kenmerken van integriteit zijn de juistheid en de volledigheid van de informatie.
- **Vertrouwelijkheid**: Vertrouwelijkheid is de mate waarin de toegang tot informatie beperkt is tot een gedefinieerde groep die daar rechten toe heeft. Hieronder vallen ook maatregelen die de privacy beschermen.

2.2 Wet- en regelgeving

De provincie Zuid-Holland heeft de relevante (inter)nationale wet- en regelgeving in kaart gebracht en voldoet aan de geldende wet- en regelgeving voor de provincie. Voor een volledig overzicht wordt verwezen naar het document 'Contextmanagement'.

[1] De termen informatieveiligheid, informatiebeveiliging en cybersecurity worden als synoniemen beschouwd.

3 Informatieveiligheid bij PZH

3.1 Visie en missie informatieveiligheid

Missie
Voor het functioneren van maatschappelijke processen en het ontwikkelen van beleidsterreinen van de provincie is een duurzame informatievoorziening en verdergaande digitalisering van processen noodzakelijk. Informatieveiligheid is een essentiële randvoorwaarde daarbij.

Visie
Om de missie te realiseren wil PZH de informatieveiligheid op orde brengen en houden door aantoonbaar te voldoen aan de ISO27001 (kantoorautomatisering), de ISO 55000 (fysieke assets) en de Baseline Informatiebeveiliging Overheid.

3.2 Strategische uitgangspunten en randvoorwaarden

Voor de beveiliging van informatie bij de provincie worden de volgende strategische uitgangspunten en randvoorwaarden gehanteerd.

- De informatieveiligheid voldoet aantoonbaar de eisen van de relevante stakeholders en aan relevante wet- en regelgeving;
- Sturing, uitvoering en controle zijn van elkaar gescheiden. Er is een proces ingericht voor de verantwoordingscyclus naar directie en bestuur;
- Door Provincie Zuid-Holland wordt gestreefd naar de continue verbetering van informatiebeveiliging. Daartoe wordt (een deel van) het security management systeem ten minste jaarlijks getoetst door middel van (interne) audits;
- Door middel van risicomanagement worden maatregelen effectief en efficiënt uitgevoerd, conform het geldende risicomanagementproces;
- Een bij de provincie passend niveau van beveiligingsmaatregelen is vastgesteld en geïmplementeerd. Het basisniveau van genomen beveiligingsmaatregelen is BBN2 conform BIO, op basis van ‘pas toe leg uit’;
- De ambtelijk opdrachtgever is verantwoordelijk voor het uitvoeren en handhaven van informatieveiligheid conform de geldende richtlijnen;
- Indien sprake is van een interne keten van informatiesystemen, is de verantwoordelijkheid van de keten onderling belegd bij één opdrachtgever;
- Bij uitbesteding controleert de ambtelijk opdrachtgever of de derde partij het door PZH vereiste betrouwbaarheidsniveau realiseert en blijft de opdrachtgever verantwoordelijk;
- Medewerkers dienen bewust te zijn van de noodzaak van de getroffen en te treffen beveiligingsmaatregelen. Medewerkers dienen over een toereikend kennisniveau te beschikken;
- Provincie Zuid-Holland stelt de benodigde resources beschikbaar om uitvoering te kunnen geven aan bovengenoemd informatieveiligheidsbeleid, zowel op het gebied van medewerkers en organisatie, als op het gebied van basisinfrastructuur en benodigde ICT-omgeving.

3.3 Organisatie van de informatieveiligheid

De volgende functionarissen dragen verantwoordelijkheid voor de informatieveiligheid.

Gedeputeerde Staten

De politieke verantwoordelijkheid voor het informatieveiligheidsbeleid behoort tot de Gedeputeerde Staten (GS). Informatieveiligheid maakt onderdeel uit van de portefeuille bedrijfsvoering. De GS stelt het informatieveiligheidsbeleid vast.

Provinciesecretaris

De provinciesecretaris is ambtelijk eindverantwoordelijk voor de inrichting en werking van de informatieveiligheid binnen de provincie. Het directieteam stelt overige beleidsdocumenten binnen de kaders van het informatieveiligheidsbeleid vast. Informatieveiligheid maakt onderdeel uit van de portefeuille van de concerndirecteur.

Ambtelijk opdrachtgever

De ambtelijk opdrachtgever is binnen zijn bevoegdheidsgebied/(beleids)opgave verantwoordelijk voor:

a. Het vaststellen van het basisbeveiligingsniveau (BBN) dat van toepassing is op het betreffende (beleids)proces conform het geldende risicomanagementproces;
b. Het bijhouden van een overzicht van kritieke systemen (‘kroonjuwelen’) voor het eigen bevoegdheidsgebied/(beleids)opgave conform een definitie van de provincie;
c. de uitvoering van het informatieveiligheidsbeleid;
d. de uitvoering van het risicomanagementproces;
e. de aansturing van de uitvoerende (overheids- of externe) organisatie die diensten levert;
f. het rapporteren over beveiligingsincidenten en de toestand van informatiebeveiliging in de jaarplancyclus;
g. het op peil houden van het beveiligingsbewustzijn van medewerkers en het stimuleren van naleving van regels en procedures;
h. het treffen van eventueel aanvullende organisatorische beveiligingsmaatregelen.

Het uitbesteden - zowel intern als extern - van diensten en processen ontslaat de ambtelijk opdrachtgever niet van zijn verantwoordelijkheid ten aanzien van informatieveiligheid.

Ambtelijk opdrachtgever Informatisering en automatisering (I&A)

De afdeling I&A heeft een verantwoordelijkheid om de basis-ICT-infrastructuur optimaal te laten functioneren op basis van het dreigings- en risicobeeld van de provincie en best practices.
De ambtelijk opdrachtgever I&A rapporteert in samenwerking met de CISO tenminste jaarlijks over risico’s en naleving van de BIO ten behoeve van de jaarlijkse directiebeoordeling.

Chief Information Security Officer (CISO)[2]

De CISO is verantwoordelijk voor de coördinatie van de informatieveiligheid met behulp van het Security Management Systeem (PDCA-cyclus). Daarnaast is de CISO verantwoordelijk voor het adviseren, monitoren en controleren van lijnmanagers/opdrachtgevers- en informatie(systeem)eigenaren in hun verantwoordelijkheden voor de beveiliging van informatie en informatiesystemen. De CISO ondersteunt daarmee de uitvoering van het digitaliseringsbeleid van de provincie.

De CISO is verantwoordelijk voor:

a) het opstellen, bijstellen, toetsen (auditen), vernieuwen en herzien van het informatieveiligheidsbeleid, het ISMS en de daaruit voortvloeiende plannen;
b) het inrichten van de informatieveiligheidsorganisatie;
c) het coördineren en adviseren bij afhandelen van (majeure) beveiligingsincidenten;
d) afstemming van informatieveiligheid met andere beveiligingsdomeinen;
e) het toezien op naleving van de eisen voor informatieveiligheid;
f) het bevorderen van het informatieveiligheidsbewustzijn over de hele organisatie;
g) de voorbereiding op toekomstige informatieveiligheidsrisico's en ICT-beveiligingsrisico's;
h) het adviseren bij en begeleiden van het risicomanagementproces en risicoanalyses;
i) het opstellen van een definitie van kritieke informatiesystemen;
j) het (laten) uitvoeren van security assessments en opdrachtgevers te adviseren over risicobeperkende maatregelen.

De CISO heeft een directe rapportagelijn naar en periodiek overleg met de (eindverantwoordelijke) provinciesecretaris en de (bestuurlijk) portefeuillehouder.

(Domein) Information Security Officer (ISO)

De domein ISO is verantwoordelijk voor de coördinatie van de informatiebeveiliging met behulp van de PDCA-cyclus binnen zijn verantwoordelijkheidsgebied.
De domein ISO is verantwoordelijk voor:

a) Bijdragen aan het opstellen, bijstellen, vernieuwen en herzien van het organisatierede informatieveiligheidsbeleid en de daaruit voortvloeiende plannen op zijn/haar domein binnen de provincie;
b) Optreden als informatieveiligheidsadviseur (voor het management) bij nieuwe informatievoorzieningen en bij ingrijpende veranderingen in de informatievoorziening;
c) Adviseren van het (lijn)management bij de uitwerking van het informatieveiligheidsbeleid in informatieveiligheidsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen;
d) Controleren van de werking en naleving van het informatieveiligheidsbeleid en daaruit voortvloeiende maatregelen;

[2] Cf. BIO norm 6.1.1.3 is er een CISO aangesteld.

e) Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de CISO.

Overige PZH-medewerkers
Medewerkers werkzaam op een PZH-locatie, met PZH-apparatuur of met PZH-informatie:
- gedragen zich conform de regels gesteld in het informatieveiligheidsbeleid;
- spreken collega's aan bij ongewenst en/of risicovol gedrag;
- melden geconstateerde of vermeende inbreuken op de beveiliging onverwijld bij de servicedesk, de ambtelijk opdrachtgever of de CISO.

3.4 Overlegstructuren informatieveiligheid

Om informatieveiligheid adequaat te kunnen sturen en monitoren is overleg op zowel strategisch als tactisch niveau noodzakelijk. Tenminste jaarlijks bespreekt de CISO de staat van de informatieveiligheid met de Concerndirecteur.

Informatieveiligheidsoverleg PZH
Het informatieveiligheidsoverleg PZH is belast met het coördineren, afstemmen en bewaken van risicomanagement en compliance onderwerpen op het gebied van informatieveiligheid. Het overleg wordt voorgezeten door de CISO en deelnemers zijn (domein) ISO's, vertegenwoordigers van fysieke veiligheid (FZ) en bescherming van persoonsgegevens (team privacy). Het overleg vindt ten minste ieder kwartaal plaats.

Informatieveiligheidsoverleg I&A
Het informatieveiligheidsoverleg I&A is belast met het coördineren, afstemmen en bewaken van risicomanagement en compliance onderwerpen binnen I&A op het gebied van informatieveiligheid. Het overleg wordt voorgezeten door de CISO en deelnemers zijn de risicomanager, en opdrachtgevers voor ICT-regie en informatiebeheer. Het overleg vindt ten minste ieder kwartaal plaats.

Overleg Informatieveiligheid en Privacy
Het overleg Informatieveiligheid en privacy is belast met de coördinatie en afstemming van werkzaamheden en beleidsontwikkelingen op de onderwerpen informatieveiligheid en privacy. Het overleg vindt tweewekelijks plaats.

4 Werkwijze

4.1 Information Security Management System (ISMS/PDCA)

Informatieveiligheid sluit zich aan bij de beleids- en rapportagecycli (PDCA-cyclus) van de provincie Zuid-Holland om de informatieveiligheidsprocessen te integraal te borgen en continu te verbeteren. Voor informatieveiligheid wordt daarvoor ten behoeve van de ICT (kantoorautomatisering) het Information Security Management System (ISMS) toegepast op basis van de ISO27001. Voor informatieveiligheid van operationele techniek wordt daarvoor ISO 55000 (assetmanagement) toegepast.

- Driejaarlijks:
  Het informatieveiligheidsbeleid van de provincie Zuid-Holland wordt elke drie jaar herzien. Het informatieveiligheidsbeleid wordt opgesteld door de CISO en vastgesteld door Gedeputeerde Staten.

- Jaarlijks:
  Op basis van het informatieveiligheidsbeleid voert de CISO een beoordeling uit van het ISMS voor de directie.

  Jaarlijks wordt een (meerjaren) voorstel voor de te auditen onderwerpen voor het ISMS opgeleverd aan de provinciesecretaris.

- Per kwartaal:
  Op basis van het informatieveiligheidsbeleid voert de CISO ieder kwartaal een tussentijdse beoordeling uit van het ISMS en risico's voor het MT I&A.

4.2 Risicomanagement

Risicomanagement stelt PZH in staat gestructureerd en verantwoord om te gaan met dreigingen, kansen en risico's. Betrouwbare bedrijfsprocessen zijn onmisbaar om de ambities en doelstellingen van de provincie te realiseren. Het is van belang dat het proces van risicomanagement cyclisch wordt ingericht en dat het niveau van integrale beveiliging regelmatig wordt herzien ten opzichte van de veranderende omgeving, dreigingen en risico's. Risicomanagement omvat het inventariseren en beoordelen van dreigingen en risico's, het besluiten over maatregelen en het tijdig uitvoeren van deze maatregelen. Gezien het volledig uitsluiten van ieder denkbaar risico onmogelijk is, blijft er altijd een restrisico bestaan. Dit restrisico dient bewust geaccepteerd te worden.

Beleid kritieke systemen ('Kroonjuwelen')
De CISO stelt een definitie op voor kritieke systemen op. Voor deze 'kroonjuwelen' van de organisatie wordt door de CISO ten minste de volgende informatie halfjaarlijks gerapporteerd aan opdrachtgever en de provinciesecretaris:

- eigenaarschap (proces en systeem) van het informatiesysteem;

- status en geldigheid van de baselinetoets;
- status en geldigheid van de risicoanalyse (als boven BBN2);
- status en geldigheid van de (pre-)privacy impact assessment;
- status van BIO implementatie;
- Datum en geldigheid security test (bv. pentest, codereview);
- Uitgevoerde en/of geplande audits (cq. inspecties);
- Status belangrijkste risico's (bv. mitigatieplan/status, acceptatie);
- Aanwezigheid en status verbeterplan.

Verantwoordelijkheden voor risicomanagement
Aanvullend op het onderscheid in verantwoordelijkheden steunt het stelsel van informatiebeveiliging op drie verantwoordelijkheidslijnen. De betreffende lijnverantwoordelijkheden werken samen in het stelsel van beveiliging en beheersing van risico's, ieder vanuit eigen verantwoordelijkheden en bevoegdheden:

- *Eerste lijnverantwoordelijkheid:*
Ambtelijk opdrachtgevers zijn verantwoordelijk voor passende informatieveiligheid van de informatiesystemen (in het bijzonder de 'kroonjuwelen') die tot hun verantwoordelijkheidsgebied of (beleids)opgave behoren.

- *Tweede lijnverantwoordelijkheid:*
Omvat de functies die ambtelijk opdrachtgevers ondersteunen en adviseren, processen coördineren en bewaken of verantwoordelijkheden daadwerkelijk worden genomen op het terrein van informatiebeveiliging, zoals de CISO of eenheid privacy waar het gaat om bescherming van persoonsgegevens.

- *Derde lijnverantwoordelijkheid:*
Partijen die onafhankelijk gepositioneerd zijn. Dit toezicht kan zowel door interne, zoals de Eenheid Audit en Advies, als door externe partijen worden uitgevoerd.