Provincie Zeeland

PROVINCIAAL BLAD

Officiële uitgave van de provincie Zeeland

Nr. 7102

30 oktober 2019

Besluit van gedeputeerde staten van Zeeland houdende Informatieveiligheidsbeleid Provincie Zeeland 2019 - 2023

Besluit van gedeputeerde staten van 22 oktober 2019, kenmerk 19426912, houdende vaststelling van het Informatieveiligheidsbeleid Provincie Zeeland 2019 – 2023.

1. Inleiding

1.1. Aanleiding en belang

De Provincie Zeeland is in toenemende mate afhankelijk van informatie en informatievoorziening. Dit is onder meer het gevolg van de steeds verdergaande digitalisering en ketenintegratie binnen de publieke sector. Uit het Cybersecuritybeeld 2018 van het Nationaal Cyber Security Centrum (NCSC) blijkt dat kwaadwillenden zich ook richten op overheden, niet alleen voor spionage maar ook voor informatiemanipulatie en sabotage. Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen van de Provincie en de betrouwbaarheid van de informatievoorziening. Door deze ontwikkelingen kunnen nieuwe kwetsbaarheden en risico's ontstaan.

Onder informatieveiligheid wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen. Deze kwaliteitsaspecten zijn van oudsher de pijlers van informatieveiligheid. Aanvullend heeft de Provincie Zeeland privacy als vierde kwaliteitsaspect toegevoegd. Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatieveiligheid is een beleidsverantwoordelijkheid van de provinciale organisatie als geheel, en is primair belegd bij Gedeputeerde Staten. Immers, onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's voor het bedrijfsproces van de Provincie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

Informatieveiligheid zelf is géén primair of secundair proces, géén kerntaak, maar als je er niets aan doet gaat het wel ten koste van de kerntaken van de organisatie: informatieveiligheid op orde is een randvoorwaarde voor een efficiënt en effectief primair proces. In bijlage 1 is de samenhang tussen het informatieveiligheidsbeleid, het privacybeleid en het informatiebeleid weergegeven.

De Provincie Zeeland heeft de ambitie om met het onderhavige beleidsdocument informatieveiligheid structureel naar minimaal het niveau van de Baseline Informatieveiligheid Overheden (BIO) te brengen. Dit niveau wordt geborgd door het opstellen, implementeren en in stand houden van een managementsysteem (ISMS) op basis van ISO27001 en het onafhankelijk laten certificeren van dit systeem in 2021.

1.2. Doel van het informatieveiligheidsbeleid

Het doel van dit beleid is het vaststellen van de organisatie van en het proces voor de beheersing van informatieveiligheid binnen de Provincie Zeeland. Het legt daarmee een basis voor:

- Het waarborgen van de veiligheid van de informatie die de Provincie verwerkt.
- Het waarborgen van de privacy van zowel burgers als medewerkers.
- Een betrouwbare bedrijfsvoering via een betrouwbare informatievoorziening.
- Het kader waarbinnen informatieveiligheid binnen de Provincie georganiseerd wordt.

Dit beleid is de richtlijn voor alle medewerkers en bestuur om veilig met informatie om te gaan. Het geeft de keuzes aan die door de Provincie Zeeland zijn gemaakt. Het beschrijft basisprincipes, verantwoordelijkheden, aanpak en rapportagelijnen.

Dit beleid is in overeenstemming met de beleidseisen uit de ISO 27001/27002 norm voor informatieveiligheid en de Baseline Informatieveiligheid Overheid (BIO) en stelt de organisatie in staat om gecertificeerd te worden op veilig omgaan met informatie.

In dit document wordt vooral de term informatieveiligheid gebruikt in plaats van informatiebeveiliging. De reden hiervoor is dat over het algemeen informatiebeveiliging een defensief en technisch karakter kent. Dit doet geen recht aan het onderwerp, waarvan de essentie is 'het veiligstellen' van informatie. Dit gebeurt net zo goed door zorgvuldig handelen in het gebruik ervan als door technische maatregelen.

Het informatieveiligheidsbeleid maakt onderdeel uit van het i-beleid van de Provincie. In bijlage 1 is de samenhang tussen de verschillende beleidsstukken weergegeven.

Het *proces* (Plan-Do-Check-Act (PDCA) cyclus) rond de beheersing van informatieveiligheid is verder uitgewerkt in het document 'Managementproces voor informatieveiligheid'. Daarnaast wordt dit beleid ondersteund door diverse beleidsdocumenten en operationele procesbeschrijvingen.

1.3 .Beheer van dit document
Dit beleid is eigendom van de portefeuillehouder Informatie en Automatisering. Het document wordt beheerd door de CISO en jaarlijks op actualiteit getoetst.

2. Informatieveiligheid

2.1. Visie op informatieveiligheid
Informatie is één van de voornaamste bedrijfsmiddelen van de Provincie Zeeland. Het verlies van gegevens en informatie, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties.

Betrouwbare en veilige informatieverwerking is dan ook zeer belangrijk, evenals de integriteit en beschikbaarheid van informatie. De Provincie Zeeland heeft dan ook een aantal strategische uitgangspunten vastgesteld om de veiligheid van informatie richting te geven. Deze uitgangspunten zijn vastgelegd in dit beleid. Het document is bindend voor alle (externe) medewerkers en leveranciers van de Provincie Zeeland.

De Provincie Zeeland is zich er daarbij van bewust dat informatieveiligheid meer behelst dan uitsluitend technische maatregelen, waar vaak als eerste aan gedacht wordt. Zorgvuldig omgaan met informatie is evenzeer een zaak van bewustwording door alle medewerkers en het afstemmen van de eigen werkwijze hierop.

In de planperiode van dit document zet de Provincie Zeeland in op het verhogen van informatieveiligheid en op verdere professionalisering van de informatieveiligheidsfunctie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de organisatie. Informatieveiligheid vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn; ieder organisatieonderdeel is hierbij betrokken. Het is de ambitie om eind 2021 gecertificeerd te zijn voor ISO27001.

2.2. Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het informatieveiligheidsbeleid zijn de volgende:

Interprovinciale Digitale Agenda
Provincies werken in gezamenlijkheid aan de Interprovinciale Digitale Agenda (IDA) met daarin verschillende sporen: innovatie, data, dienstverlening en bedrijfsvoering. Samenwerking staat daarbij centraal. Daarnaast wordt aangesloten op de digitale agenda's van andere bestuurslagen waarmee wordt samengewerkt. De digitale transformatie, die in de gehele maatschappij gaande is, biedt kansen maar levert tegelijkertijd ook risico's op die onderkend moeten worden. De Provincie moet enerzijds in staat zijn om informatie adequaat te kunnen delen met keten- en netwerkpartners en anderzijds hierbij kritisch te zijn in relatie tot informatieveiligheid.

Nieuwe wetgeving: Wet Open Overheid, Wet Elektronische Bekendmakingen en de Omgevingswet
De Wet Open Overheid vraagt een open en transparante informatievoorziening, zowel intern als extern (vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren). De Wet Elektronische Bekendmakingen richt zich op het volledig elektronisch bekendmaken van publicaties. De Omgevingswet zal een impuls geven om de organisatie meer integraal te laten werken. Er worden twee belangrijke onderdelen onderscheiden, namelijk het Digitaal stelstel Omgevingswet en diverse informatieproducten die eventueel in een later stadium zullen worden ontsloten via zogenaamde informatiehuizen.

Samenwerking
De Provincie werkt in toenemende mate samen met verschillende (keten)partners. Uitwisseling van informatie in verschillende vormen is daarbij een onlosmakelijk onderdeel. In dit kader worden ook

gezamenlijk met partners of zelfstandig informatieproducten ontwikkeld, waarbij het gebruik van (cloud)diensten van derden toeneemt. De verkenning van een provinciaal datacentrum dat (mogelijk) wordt opgezet in samenwerking met de gemeenten en het CBS is daar een belangrijk voorbeeld van. Verder wordt op interprovinciaal niveau samenwerking gezocht op het gebied van data en applicaties (GBO). Tenslotte zijn er initiatieven om op het gebied van ICT dienstverlening (kantoorautomatisering) samen te werken met één of een aantal regionale partners. Voor beide vormen van samenwerking is het van belang dat informatieveiligheid een integraal onderdeel vormt van de werkwijze en te maken afspraken daarover.

Cloud beleid
In algemene zin is er een ontwikkeling in gang gezet waarbij een toenemend aantal informatiesystemen via SAAS (software as a service) oplossingen worden afgenomen van leveranciers, de Provincie anticipeert hier al een aantal jaren opbij nieuwe ontwikkelingen. Dit impliceert dat een deel van de informatie op andere locaties is opgeslagen dan de serverruimten binnen de Abdij en het Waterschapsgebouw. Het is van belang dat er passende afspraken gemaakt worden met leveranciers ten aanzien van betrouwbaarheid, integriteit en vertrouwelijkheid van deze informatie en dat op naleving hiervan ook wordt toegezien.

Baseline Informatieveiligheid Overheden (BIO)
Overheden hebben onderling afgesproken dat zij met ingang van 1 januari 2020 voldoen aan de maatregelen zoals omschreven in de baseline informatieveiligheid overheden (BIO). Deze baseline is gebaseerd op de maatregelen uit ISO27002. In 2018 is een gap analyse uitgevoerd op basis waarvan duidelijk is geworden welke maatregelen er door de Provincie Zeeland nog moeten worden getroffen. In combinatie met het project implementatie ISO27001 wordt aan de implementatie van de benodigde maatregelen gewerkt.

Project Versterking Interne Beheersing
Binnen de organisatie is het project 'Versterking Interne Beheersing' gestart. Met het informatieveiligheidsbeleid en de uitwerking daarvan, wordt aangesloten bij dit project.

2.3. Risico-gebaseerde benadering van informatieveiligheid

De Provincie Zeeland definieert veilig omgaan met informatie als het proces van het beschermen van informatie en gerelateerde componenten (zoals geautomatiseerde informatiesystemen, personen en papieren documenten) tegen onbedoelde of vooropgezette inbreuken van:

- **Beschikbaarheid**: Informatie dient beschikbaar te zijn op het moment dat het nodig is, wat eisen stelt aan de beschikbaarheid van informatiesystemen en databases.
- **Integriteit**: De gebruiker moet erop kunnen vertrouwen dat informatie juist, volledig, tijdig en geoorloofd is. Handhaving hiervan is verankerd in procesafspraken, maar ook in maatregelen die ongeoorloofde of ongewenste (expres of per ongeluk) mutaties tegengaan.
- **Vertrouwelijkheid**: Gebruikers en belanghebbenden moeten er op kunnen vertrouwen dat informatie alleen beschikbaar is voor die gebruikers die het nodig hebben voor de uitvoering van hun functie en niet onnodig ter inzage van anderen is.
- **Privacy**: Als bijzondere vorm van Vertrouwelijkheid, welke wettelijk is gereguleerd via de AVG: lekken van burgergegevens en/of van klanten raakt direct de reputatie van de Provincie. Lekken van persoonsgegevens roept extra aandacht van de Autoriteit Persoonsgegevens op, die kan dwingen tot kostbare maatregelen en eventueel een boete.

Veilig omgaan met informatie richt zich op de bescherming van informatie tegen bedreigingen en gaat in principe over de beantwoording van drie vragen:

1. Wat zijn mijn meest waardevolle gegevens en informatiesystemen?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze meest waardevolle gegevens en informatiesystemen?
3. Wat ga ik wel en niet doen om mijn gegevens en informatiesystemen beschermen tegen deze gebeurtenissen?

De Provincie hanteert derhalve een risico-gebaseerde benadering, waarbij op basis van een risicoanalyse op procesniveau maatregelen worden getroffen. Zowel zakelijke overwegingen (kosten en baten) als externe verplichtingen worden in deze benadering meegenomen. Maatregelen staan steeds in verhouding tot de bedrijfsprocessen van de Provincie en de eisen aan de continuïteit hiervan. Eventuele restrisico's worden expliciet door de organisatie geaccepteerd.

2.4. Wet- en regelgeving

Bij het opstellen van dit beleid is in ieder geval rekening gehouden met de eisen die gesteld worden in de onderstaande wet- en regelgeving. Dit overzicht wordt getoetst bij de periodieke herziening van dit beleidsdocument.

a) Algemene Verordening Gegevensbescherming (AVG)
b) Regeling meldplicht Datalekken
c) Aanwijzingsbesluit verwerking personeelsgegevens
d) Wet beveiliging netwerk- en informatiesystemen
e) Standaarden Forum voor Standaardisatie
f) Wet Openbaarheid Bestuur
g) Archiefwet en Archiefregeling
h) Baseline Informatieveiligheid Overheid (BIO)
i) Wet open overheid
j) Wet elektronische bekendmakingen
k) Omgevingswet

Verder bestaat het wettelijk kader meer algemeen uit: de Grondwet, de Ambtenarenwet en de Collectieve Arbeidsvoorwaardenregeling Provincies (CAP) en diens opvolger CAO Provinciale sector.

2.5. Reikwijdte

Dit beleid heeft betrekking op de totale informatievoorziening van de interne organisatie van de Provincie, zowel kantoor- als procesautomatisering, van de Provincie Zeeland inclusief de werkomgeving van het provinciaal bestuur (Commissaris van de Koning en Gedeputeerde Staten), de internetomgeving, mobiele apparaten en thuiswerkvoorzieningen. Het beleid heeft ook betrekking op informatie in bijvoorbeeld papieren dossiers, mobiele computers, USB-sticks, smartphones, tablets en dergelijke. De geautomatiseerde gegevensuitwisseling met externe organisaties, informatiesystemen in beheer bij derde partijen en de ontwikkeling van informatiesystemen vallen ook binnen de scope van dit beleid

Het beleid is van toepassing op de werklocaties van de Provincie Zeeland:

- Kantoorcomplex Abdij 6 Middelburg;
- Waterschapskantoor Kanaalweg 1 in Middelburg;
- de Nautische Centrale Vlissingen (waar ook de brug- en sluisbediening is gesitueerd);
- de wegensteunpunten.

Het informatieveiligheidsbeleid dient door medewerkers van alle organisatieonderdelen te worden opgevolgd, ongeacht de locatie waar men werkt.

2.6. Opzet en geldigheid

Dit beleid wordt vastgesteld door het college van Gedeputeerde Staten (GS). De geldigheid van dit document is vastgesteld op 4 jaar vanaf de datum van inwerkingtreding. Daarna wordt jaarlijks een evaluatie uitgevoerd om na te gaan of dit beleid voortgezet of aangepast dient te worden.

Informatieveiligheid is een dynamisch proces. Dit is het gevolg van voortdurende organisatorische, juridische en technologische veranderingen. Op basis van dit algemeen beleidskader worden specifieke organisatie eigen richtlijnen en beheersmaatregelen per categorie uitgewerkt. De Chief Information Security Officer (CISO) is verantwoordelijk voor het voorstellen van wijzigingen of aanvullingen. Tevens zorgt hij voor het inbrengen van deze zaken in de betreffende management overleggen.

3. Uitgangspunten voor informatieveiligheid

De Provincie Zeeland hanteert een kader voor de inrichting en verdere uitwerking van informatieveiligheid. De onderstaande uitgangspunten worden daarbij gehanteerd. Dit kader dient als leidraad wanneer er zich vraagstukken voordoen op het gebied van informatieveiligheid die niet nog verder zijn uitgewerkt.

1. Veilig omgaan met informatie is een **verantwoordelijkheid** van alle medewerkers in de hele organisatie.
2. **Het management is primair verantwoordelijk** voor de invoering en handhaving van informatieveiligheid binnen de onderscheiden organisatie onderdelen en stelt medewerkers in staat hun verantwoordelijkheid te nemen.

3. Ieder proces, informatiesysteem, gegeven en generieke infrastructuur (fysiek en informatie) heeft één **formele eigenaar** op managementniveau.
4. De Provincie heeft een aantal **standaard maatregelen** getroffen, waarmee een basisniveau voor informatieveiligheid wordt geboden. Deze maatregelen worden op drie functionele gebieden aangeboden door de afdelingen POJZ, I&A en FAC, uitgewerkt in catalogi met standaard diensten (zie bijlage 1 voor schema samenhang beleidsproducten).
5. Maatregelen zijn in **balans** met de te beschermen waarde; dit betekent dat onderzoek gedaan moet worden naar de noodzaak van maatregelen. De Provincie Zeeland gebruikt hiervoor een **risicoanalyse**. Risicomanagement is onderdeel van de besluitvorming.
6. **Informatie is intern vrij beschikbaar** voor medewerkers, tenzij de beveiligingsclassificatie van deze informatie anders voorschrijft. Het verantwoordelijk lijnmanagement geeft op basis van de beveiligingsclassificatie van de informatie medewerkers autorisatie voor fysieke en logische toegang.
7. Informatieveiligheid wordt ook meegenomen bij het opzetten en uitvoeren van **(keten)samenwerking**. Ook hierbij wordt risicomanagement toegepast.
8. Er wordt planmatig gewerkt aan het verhogen en borgen van **bewustwording en kennis** van alle medewerkers op het gebied van informatieveiligheid en privacy. Er worden structureel middelen ter beschikking gesteld voor opleiding, communicatie en training. Trainingen m.b.t. de beginselen van veilig werken bij de Provincie Zeeland worden verplicht voor management en medewerkers.

Daar waar afgeweken wordt van een vastgesteld beleid of standaarden, legt het management of de proceseigenaar dit vast in een formele verklaring (‘comply or explain’). De verklaring bevat een risico-inschatting van de afwijking en de mogelijke consequenties en wordt aan de CISO gerapporteerd. Afwijkingen zijn alleen toegestaan na uitvoering van een risicoanalyse en met schriftelijke toestemming van de bestuurder.

4. Organisatie van Informatieveiligheid

4.1. Taken, verantwoordelijkheden en bevoegdheden

Informatieveiligheid is op vier niveaus ingericht en geborgd, waarbij elk niveau een eigen verantwoordelijkheid heeft.

Niveau	Verantwoordelijkheid (globaal)	Verantwoordelijke rol
Besturend	Bepalen van de ambitie en het beleid Invullen randvoorwaarden voor invoering van het beleid	Gedeputeerde Staten Directie
Coördinerend	Overzicht houden op voortgang invoering en ontwikkeling van beleid en richtlijnen	CISO Projectgroep informatieveiligheid
Handhavend	Uitvoering en handhaving van beleid en richtlijnen Herkennen en bewaken van de risico’s	CISO Lijnmanagement
Uitvoerend	Uitvoering van beleid en richtlijnen	Medewerkers Lijn management

- *Gedeputeerde Staten (GS)*
  GS stellen het informatieveiligheidsbeleid vast. GS zijn het hoogste besluitvormend gremium voor Informatieveiligheid en privacy. De Provincie kent een collectieve bestuurlijke verantwoordelijkheid. GS maken in het kader van de Planning & Control-cyclus afspraken met de aan hen rapporterende managers over de uitvoering van het informatieveiligheidsbeleid en het toezicht hierop en stelt de noodzakelijke middelen beschikbaar.

- *De directie*
  De directie is strategisch eindverantwoordelijk voor de informatieveiligheid van de organisatie. De directie legt de verbinding met het bestuur bij calamiteiten.

- *De Chief Information Officer (CIO)*
  De organisatiebrede rol van CIO wordt ingevuld door de afdelingsmanager Informatie en Automatisering. De CIO adviseert directie en bestuurders over de strategie rond informatieveiligheid en zorgt voor de noodzakelijke middelen. De CIO houdt toezicht op de uitvoering en implementatie van het beleid voor informatieveiligheid en is verantwoordelijk voor het functioneren van het managementproces rond informatieveiligheid (PDCA-cyclus). Het betreffende document (managementproces voor informatieveiligheid) wordt jaarlijks geactualiseerd en door de CIO vastgesteld. De CIO is verantwoordelijk voor acceptatie van rest risico’s.

- *De Chief Information Security Officer (CISO)*
  De CISO coördineert, bewaakt en neemt deel aan de uitvoering van het managementproces rond informatieveiligheid (PDCA-cyclus). De CISO ontwikkelt, in samenwerking met de uitvoerende organisatieonderdelen, operationele richtlijnen en procedures voor informatieveiligheid en continue verbetering. De CISO coördineert en bewaakt de uitvoering van het informatieveiligheidsbeleid en verhoogt en houdt het bewustzijn rond informatieveiligheid op peil door het opstellen en uitvoeren van een bewustwordingsplan. De CISO ondersteunt de organisatie met gevraagd en ongevraagd advies.

- *De projectgroep Informatieveiligheid*
  De projectgroep informatieveiligheid ondersteunt de CISO bij het uitvoeren van de taken en zorgt door zijn samenstelling voor een continue verbinding van de organisatie bij de inspanningen op het gebied van informatieveiligheid.

- *De functionaris gegevensbescherming (FG)*
  De FG houdt onafhankelijk toezicht op de naleving van de AVG door de Provincie. Daarnaast geeft hij gevraagd en ongevraagd advies over onderwerpen en kwesties die de privacyrechten raken van inwoners of de medewerkers van de Provincie. De FG coördineert en bewaakt de uitvoering van het privacybeleid en de protocollen voor gegevensverwerking en datalekken. Samen met de CISO houdt de FG de bewustwording onder collega's op peil om te handelen volgens de AVG-principes en informatieveiligheid. De FG wordt ondersteund door de projectgroep AVG.

- *De Provinciearchivaris*
  De Provinciearchivaris heeft onafhankelijk toezicht op het niet overgebrachte deel en vanuit die hoedanigheid houdt hij ook toezicht op de informatieveiligheid. Hij rapporteert schriftelijk de bevindingen en aanbevelingen eens per twee jaar rechtstreeks aan de colleges van GS en PS.

- *Het management*
  Het management is eindverantwoordelijk voor informatieveiligheid binnen zijn/haar organisatieonderdeel (afdelingen, opgave of programma). De belangrijkste taak is om in de dagelijkse praktijk toe te zien op de naleving van het beleid en de gemaakte afspraken rond informatieveiligheid door de medewerkers. Daarnaast houdt het management in het oog welke risico's bestaan en ontstaan en hoe daarvoor praktische maatregelen voor te treffen. Het management werkt daarbij nauw samen met de applicatie- en proceseigenaren.

- *De informatiesysteem- en proceseigenaren*
  De informatiesysteem- en proceseigenaren zijn verantwoordelijk voor het uitvoeren van risicoanalyses op processen en onderliggende applicaties en informatiesystemen, zorgen voor vaststelling van bijbehorende beveiligingsmaatregelen en acceptatie van restrisico's. Daarnaast zorgen zij ervoor dat de digitale informatie wordt geclassificeerd conform de gehanteerde classificatiemethodiek en dat de naleving van de relevante maatregelen wordt getoetst. Ze worden hierbij gefaciliteerd door de CISO, de architecten, de werkgroepleden informatiebeveiliging, de provincieadvocaat, functioneel applicatiebeheerders en key users.

- *De medewerkers*
  Alle medewerkers (inclusief uitzendkrachten, stagiaires etc.) van de Provincie zijn zich bewust van het beleid en de onderliggend richtlijnen en procedures en handelen daarnaar. Hierin worden zij gestuurd door hun leidinggevenden en geadviseerd door de projectgroep informatieveiligheid en de CISO. Bij (noodzakelijke) registratie van tot personen herleidbare gegevens moet worden voldaan aan de AVG. In de jaargesprekken is aandacht voor informatieveiligheid.

- *Externe partijen*
  Alle externe partijen die worden ingehuurd, bijvoorbeeld voor ICT-werkzaamheden, beveiliging en consultants zijn gehouden aan het informatieveiligheidsbeleid. Op basis van een risicoanalyse dienen adequate maatregelen te worden genomen om geheimhouding van informatie zo goed mogelijk te borgen.

4.2. Overleg- en rapportagestructuren informatieveiligheid

De CISO rapporteert en geeft gevraagd en ongevraagd advies aan de directie en (de portefeuillehouder van) GS. GS is het hoogste besluitvormend gremium voor Informatieveiligheid.

Overleg	Frequentie
Portefeuillehouder GS – CIO & CISO	Tenminste eens per half jaar
CIO – CISO	Tenminste eens per 6 weken
CISO – Projectteam Informatieveiligheid	maandelijks
Directie – CISO (managementbeoordeling)	jaarlijks
GS – CISO + CIO (managementbeoordeling)	jaarlijks

De rapportage van de CISO volgt verder het stramien van de P&C cyclus en de kwartaalrapportages (waaronder de provinciale risicorapportage).

5. Naleving en evaluatie

Veiligheidsmaatregelen worden getroffen om risico's te verminderen. Om de controle over de risico's te waarborgen is het noodzakelijk regelmatig na te gaan of maatregelen nog werken en nog steeds de beoogde veiligheid bieden. Naast de dagelijkse interne controle door de lijnorganisatie en bewaking door de CISO, is in de interne auditcyclus en –planning van het unit Control ook informatieveiligheid meegenomen. Dit gebeurt in samenwerking met de CISO. Daar waar het onderwerp van audit specifieke kennis vraagt, huurt de Provincie externe capaciteit in.

De Provincie Zeeland zal eind 2021 ISO27001 gecertificeerd zijn. Vanaf dat moment wordt elke drie jaar een hercertificeringsaudit uitgevoerd en wordt elk jaar een opvolgingsaudit uitgevoerd.

Daarnaast vinden periodiek externe, onafhankelijke audits periodiek plaats door de accountant. Bevindingen op het gebied van informatieveiligheid worden afgestemd met en mede bewaakt door de CISO.

Aldus vastgesteld in de vergadering van gedeputerde staten van 22 oktober 2019.

Drs. J.M.M. Polman, voorzitter

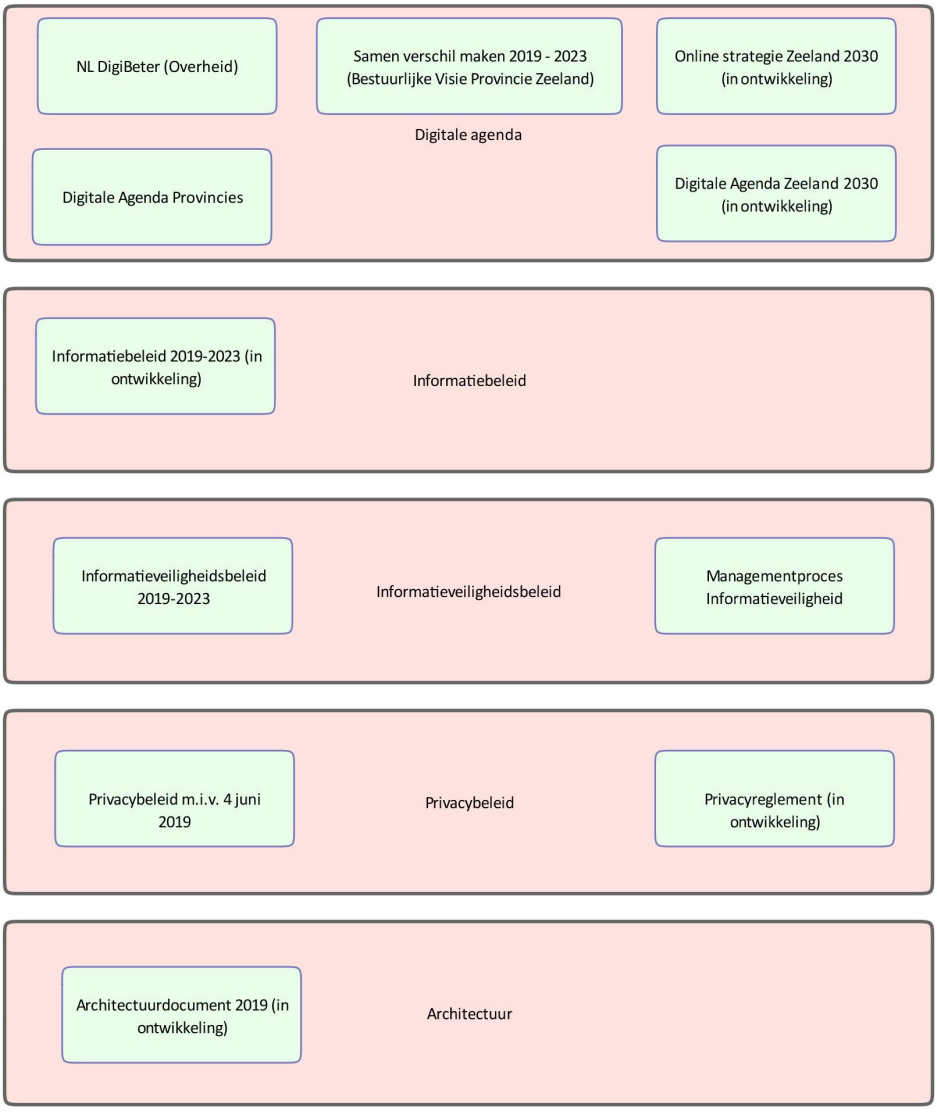
A.W. Smit, secretaris

Uitgegeven, 30 oktober 2019

De secretaris, A.W. Smit

Bijlage 1: Samenhang producten i-beleid Provincie

Name: Samenhang Informatiebeleid Provincie Zeeland
Author: IA/ VKA
Version: 1.2
Created: 19-9-2019 00:00:00
Updated: 23-9-2019 15:03:41



De afbeelding geeft schematisch de samenhang weer van het informatieveiligheidsbeleid met het informatiebeleid van de Provincie Zeeland. De digitale agenda, het informatiebeleid, het privacy beleid en de architectuur vormen met het informatieveiligheidsbeleid het beleidskader voor informatievoorziening van de Provincie.
De digitale agenda bestaat uit de online strategie Zeeland 2030, de bestuurlijke visie (Samen verschil maken 2019-2023), de Digtale agenda Provincies en NL Digibeter. Binnen het privacy beleid valt ook het privacy reglement: deze is nog in ontwikkeling. Het architectuurdocument wordt in 2019 herzien.