Omgevingsdienst Zuid-Holland Zuid

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1130

16 november 2020

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid

Strategisch Informatiebeveiligingsbeleid Omgevingsdienst Zuid-Holland Zuid 2020 - 2024

Vastgesteld door het dagelijks bestuur op 13 november 2020

1. INLEIDING

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2024. Het beleid is gebaseerd op het Strategisch Informatiebeveiligingsbeleid Drechtsteden 2020 tot 2024 en vervangt de paragrafen over informatiebeveiliging in het Privacy- en informatiebeveiligingsbeleid Omgevingsdienst Zuid-Holland Zuid uit 2018.

Het Strategisch informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. Het wordt aangevuld met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten. Met dit beleid zet OZHZ een volgende stap om de beveiliging van persoonsgegevens en andere informatie te continueren en voort te gaan op de stappen die in de voorgaande jaren zijn gezet. De basis voor dit beleid is de NEN-ISO/IEC 27001:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO, Staatscourant 19 april 2019). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging, zoals op 30 november 2018 vastgesteld door de Vereniging van Nederlandse Gemeenten (VNG).

Informatiebeveiliging gaat over het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. Het beleid geldt voor alle processen van OZHZ en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en het karakter van de informatie. Het beperkt zich niet alleen tot de ICT maar heeft ook betrekking op het bestuur, de medewerkers, inwoners, bezoekers en externe relaties.

OZHZ trekt bij informatiebeveiliging samen op met de organisaties binnen de Drechtsteden. Samen is ook de volgende ambitie en visie voor informatiebeveiliging geformuleerd:
'Wij werken duurzaam veilig, nu en in de toekomst zodat innovatie helpt onze doelen te realiseren".

Deze ambitie en visie ligt ten grondslag aan dit beleidsdocument.

2. STRATEGISCH BELEID

2.1 Doel

Dit document bevat het Strategisch Informatiebeveiligingsbeleid Omgevingsdienst Zuid-Holland Zuid 2020 - 2024. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks vast te stellen Jaarwerkplan informatiebeveiliging.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende.

2.2.1 De BIO
De Baseline Informatiebeveiliging Overheid(BIO) is het nieuwe normenkader voor de gehele overheid. De werkwijze van de BIO is meer dan het oude normenkader (de BIG) gericht op risicomanagement. Dat wil zeggen dat de procesverantwoordelijken nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001, en daarbij is risicomanagement van belang. De unitmanagers gelden binnen OZHZ als procesverantwoordelijken. Dit houdt in dat zij op voorhand keuzes en continu afwegingen maken of informatie in de bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Daarnaast geldt dat OZHZ NEN-EN-ISO 9001-2015 gecertificeerd is, en dus ook aan dit normenkader moet voldoen.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO en gaan over de waarden die het bestuur zichzelf oplegt:
1. Het bestuur bevordert een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.
De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen het bestuur en de directie bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor klanten, inwoners, ondernemers en partners van de organisatie. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 Resultaatgebieden
Tien resultaatgebieden bieden de organisaties in de Drechtsteden, waaronder OZHZ, de mogelijkheid om op de invoering van de verplichte en gekozen maatregelen te sturen. De resultaatgebieden zijn als volgt.

Risicomanagement
De organisaties in staat stellen om een duidelijk beeld te krijgen op informatiebeveiligingsrisico's en hoe de risicobereidheid door maatregelen kunnen worden afgedekt.

Kennis en bewustzijn
Het is belangrijk dat de volledige organisatie en in het bijzonder de informatiebeveiligingsadviseurs de kennis en kunde krijgen om hun taak op een goede manier uit te voeren. Verspreiding van kennis en bewustwording zal door Chief Information Security Officer (CISO) en de informatiebeveiligingsadviseurs plaats moeten gaan vinden op strategisch, tactisch en operationeel niveau.

Compliance management
De organisaties in staat stellen grip te houden op hoe de systemen en applicaties zijn geïmplementeerd. Hierbij wordt gekeken of ze voldoen aan de gestelde eisen en welke risico's eventueel voortkomen uit discrepanties.

Klantbeleving
Informatiebeveiliging dient een positief gevoel te geven bij medewerkers en dient hen te ondersteunen in hun dagelijkse werk.

Innovatiemanagement
Informatiebeveiliging is een onderwerp dat net zoveel met de toekomst te maken heeft als met het verleden. Het is daarom belangrijk om vanuit een informatiebeveiligingsperspectief vernieuwing en innovatie te ondersteunen om zo klaar te zijn voor de toekomst.

Leveranciers en contractmanagement
Met de huidige push naar sourcing vanuit het ICT-transitieplan van de Gemeenschappelijke regeling Drechtsteden en de sourcingstrategie wordt het essentieel om op strategisch niveau contacten te hebben en te onderhouden met de belangrijke leveranciers. Dit om te zorgen dat ook naar de toekomst toe de informatiebeveiliging kan worden geborgd.

Informatiemanagement
Informatiebeveiliging en informatiemanagement zijn sterk met elkaar verbonden en kunnen niet zonder elkaar. Met een juiste toepassing van informatiemanagement wordt er in de beginfase van het voortbrengingsproces al aandacht gevestigd op Privacy by Design en Security by Design.

Incidenten- en crisismanagement
Indien zich grote incidenten voordoen of een crisissituatie ontstaat dient informatiebeveiliging hierbij te ondersteunen.

Advies
Gevraagd en ongevraagd zal vanuit het CISO-team advies worden gegeven.

Security Governance
Het duidelijk neerzetten van een governance structuur is belangrijk. De organisatie moet eigenaarschap hebben belegd en verantwoordelijkheid nemen voor de risico's die worden gelopen en de maatregelen die worden getroffen.

2.2.4 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel beeld van incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.5 Informatie uit incidenten en inbreuken op de beveiliging
De samenwerkende organisaties in de Drechtsteden kennen naast het hierboven genoemde dreigingsbeeld ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem van het Servicecentrum Drechtsteden geeft waardevolle informatie om van te leren. Incidenten uit het verleden zijn dus nadrukkelijk input bij het actualiseren van het regiobrede beleid.

2.3 Standaarden voor informatiebeveiliging

De basis voor de inrichting van het beleid is NEN-ISO/IEC 27001:2017. De maatregelen worden genomen op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017.

Voor de ondersteuning van alle overheden bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke Werkgroep Normatiek, bestaande uit vertegenwoordigers van de VNG, de IBD, waterschappen, provincies en het rijk, in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze nota zijn afgestemd op die van de NEN-ISO en de BIO.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactisch beleid en tactische beleidsplannen, en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Deze nota beschrijft het informatiebeveiligingsbeleid op strategisch niveau, en zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden werkt OZHZ uit in het Jaarwerkplan informatiebeveiliging.

2.5 Scope van de informatiebeveiliging

De scope van dit beleid omvat alle werkprocessen binnen OZHZ, de onderliggende informatiesystemen, informatie en gegevens van de dienst en van externe partijen (bijvoorbeeld van de Veiligheidsregio en de Dienst Gezondheid en Jeugd en van de gemeenten en de provincie), het gebruik ervan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Dit strategisch informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP.

Dit strategisch regionale Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit (nieuwe) wetgeving af, zoals onder andere uit de Algemene Verordening Gegevensbescherming (AVG), de Wet basisregistratie personen (BRP), de Wet Basisregistratie adressen en gebouwen (BAG), de Wet basisregistratie ondergrond (BRO) en DigiD.

Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen Deze worden in aanvullende documenten geformuleerd. Lokale handboeken zijn aanvullend op dit beleid; de daarin genoemde aanvullende beveiligingseisen zijn leidend. Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt wel de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur, de directie en de procesverantwoordelijken spelen een cruciale rol bij het uitvoeren van dit beleid. De unitmanager maakt een inschatting van het belang dat de verschillende delen van de in-

formatievoorziening (zoals een bepaalde applicatie) voor de unit en de organisatie hebben, de risico's die de unit en de organisatie hiermee lopen en welke van deze risico's onacceptabel hoog zijn.

Op basis vertaalt de unitmanager dit informatiebeveiligingsbeleid naar operationele spelregels, draagt dit uit naar de unit en de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en laat zien dat het informatiebeveiliging ondersteunt en zich hierbij betrokken voelt. Dit door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie. Het beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid binnen OZHZ en de Drechtsteden en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid zijn:
1. Het managen van de informatiebeveiliging.
2. Adequate bescherming van bedrijfsmiddelen.
3. Het minimaliseren van risico's van menselijk gedrag.
4. Het voorkomen van ongeautoriseerde toegang.
5. Het garanderen van correcte en veilige informatievoorzieningen.
6. Het beheersen van de toegang tot informatiesystemen.
7. Het waarborgen van veilige informatiesystemen.
8. Het adequaat reageren op incidenten.
9. Het beschermen van kritieke bedrijfsprocessen.
10. Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
11. Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
• Alle informatie en informatiesystemen zijn van belang voor de organisatie. Bepaalde informatie is van vitaal en kritiek belang.
• Het dagelijks bestuur is eindverantwoordelijke voor de informatiebeveiliging.
• De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van de procesverantwoordelijke. Alle informatiebronnen en -systemen die OZHZ gebruikt hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
• Door periodieke controle, organisatiebrede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het Jaarwerkplan informatiebeveiliging het fundament onder een betrouwbare informatievoorziening. In het Jaarwerkplan informatiebeveiliging wordt de betrouwbaarheid van de informatievoorziening in samenhang met de regio breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
• Informatiebeveiliging is een continu verbeterproces. Plan, do, check en act vormen samen het managementsysteem van informatiebeveiliging.
• De organisatie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
• Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
• Iedere medewerker en/of gebruiker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
• Het dagelijks bestuur stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
• De directie stelt het Jaarwerkplan informatiebeveiliging vast. De directie is ook verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
• De directie is verantwoordelijk voor het vragen om informatie bij de procesverantwoordelijken en ziet erop toe dat zij adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
• De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.

• Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging naar aanleiding van de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
• De procesverantwoordelijken zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen binnen hun unit en worden daarbij ondersteund door de informatiebeveiligingsmedewerker van OZHZ.
• Hoewel de basiskernregistraties (zoals BRP en BAG) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de organisatie. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de organisatie en het behalen van de doelen die zijn gesteld.
• Alle medewerkers van de organisatie worden getraind in het gebruik van beveiligingsprocedures.
• Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
• De unitmanagers zien erop toe dat de controle op het juist verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens verwerken.
• De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Procesverantwoordelijken voeren quickscans (basisrisicoanalyses ofwel BRA's) informatiebeveiliging uit op basis van de BIO om deze risicoafwegingen te kunnen maken.

2.6.4 Randvoorwaarden
Belangrijke randvoorwaarden zijn als volgt.

Contractbeheer
De informatiebeveiliging maakt deel uit van afspraken met ketenpartners. In verwerkersovereenkomsten met externe verwerkers is het normenkader BIO als vereiste opgenomen.

Bewustwording
Kennis en bewustzijn van informatiebeveiliging en specifiek omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.

Risicomanagement
Jaarlijks stelt OZHZ een werkplan over informatiebeveiliging op, in afstemming met de CISO. Dit plan is gebaseerd op:
• De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) van de gemeenten.
• Het dreigingsbeeld gemeenten van de IBD.
• Een gezamenlijke sessie over risicomanagement, georganiseerd door de CISO met input van informatiebeveiligingsadviseurs van de organisaties in de Drechtsteden.
• De door de procesverantwoordelijken van de organisaties in de Drechtsteden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

Middelen
Voor de uitvoering van het informatiebeveiligingsbeleid is capaciteit en budget beschikbaar om de uitgangspunten, maatregelen en bevindingen te kunnen implementeren.

3. ORGANISATIE, TAKEN EN VERANTWOORDELIJKHEDEN

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model zijn de proceseigenaren verantwoordelijk voor de eigen processen. De tweede lijn (CISO, informatiebeveiligingsadviseur van OZHZ) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directie

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een procesverantwoordelijke. De directie zorgt dat de procesverantwoordelijken zich verantwoorden over de beveiliging van de informatie die onder hen berust.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Zij draagt ook zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO en de informatiebeveiligingsadviseur van OZHZ. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt gezien als een integraal onderdeel van risicomanagement.

De directie zorgt dat het dagelijks bestuur gevraagd en ongevraagd wordt geïnformeerd over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het dagelijks bestuur zich ook verantwoorden naar het algemeen bestuur en naar de deelnemers in de gemeenschappelijke regeling.

3.2 Uitvoering: de unitmanagers zijn procesverantwoordelijk

Informatiebeveiliging valt onder de verantwoordelijkheid van de procesverantwoordelijken. Binnen OZHZ zijn dat de unitmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. De verantwoordelijkheid kunnen zij niet delegeren, de uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data en applicaties altijd één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Procesverantwoordelijken rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de betrokkenen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het directieteam en het gezamenlijke overleg van de unitmanagers.

Taken van de unitmanagers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op procedures en maatregelen.
- Uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures en maatregelen binnen de unit.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld onder andere door het uitvoeren van quickscans of basisrisicoanalyses.
- Bespreken van beveiligingsincidenten en de consequenties die dit moet hebben voor het beleid en de maatregelen.

3.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het dagelijks bestuur van OZHZ. De directeur en de unitmanagers van OZHZ zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het laten zien van voorbeeldgedrag en het vragen om informatie. De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het dagelijks bestuur. De unitmanagers rapporteren daarnaast over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel-) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

Gemeenten verantwoorden zich over informatiebeveiliging middels de landelijk beschikbaar gestelde zelfevaluatie tool (ENSIA). Voor deze zelfevaluatie en het daaropvolgend auditproces wijzen zij een coördinator aan. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van de vragen wordt opgehaald bij de procesverantwoordelijken. De procesverantwoordelijken leveren alle informatie die nodig is voor het invullen van de zelfevaluatie. De ingevulde vragenlijst vormt voor de gemeenten de basis voor het opstellen van de collegeverklaring voor zowel de horizontale als verticale verantwoording. De betrokkenheid van het bestuur is essentieel. Daarmee laat het zien dat het informatiebeveiliging serieus neemt en dat het een onderdeel laat zijn van de ambities om informatie adequaat te beschermen.

OZHZ rapporteert over de uitvoering van het Privacybeleid en van het Informatiebeveiligingsbeleid in de jaarstukken van de gemeenschappelijke regeling. Deze worden door het algemeen bestuur vastgesteld. Informatiebeveiliging is ook onderdeel van de jaarlijkse audit van de Functionaris Gegevensbescherming (FG). De directie agendeert de rapportage van de FG in het dagelijks en algemeen bestuur en vermeld daarbij welke acties worden opgepakt om invulling te geven aan de aanbevelingen van de FG.