Strategisch Informatiebeveiligingsbeleid Drechtsteden

2020 tot 2024

20-05-2020

Tom de Haan (CISO) / Arjan Meijer (CISO)

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.99	19-05-2019	Tom de Haan / Arjan Meijer	Aanpassingen Drechtsteden
	26-7-2019	Ben Giltjes en Gina van den Broek	Aanpassingen
	7-8-2019	PIO-D	Aanpassingen
1.00	20-05-2020	PIO-D	Finale afstemming

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2024 en vervangt het in 2015 en 2019 vastgestelde Informatiebeveiligingsbeleid Drechtsteden. Het Strategisch informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument en wordt aangevuld met beleid voor informatiebeveiliging op tactisch - en operationeel niveau met specifieke (beleids)documenten.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2020-2024' zet de Drechtsteden een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de Drechtsteden te continueren en voort te gaan op de stappen die in de voorgaande jaren zijn gezet. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27001:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)[1]. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging [2]zoals vastgesteld door de Vereniging van Nederlandse Gemeente (VNG).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels. In het jaarlijks uit te brengen Informatiebeveiligingsplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de deelnemende organisaties, risicoanalyses, de rapportage van de Chief Information Security Officer (CISO), het dreigingsbeeld van de Informatiebeveiligingsdienst (IBD), de uitkomsten van zelfevaluaties en audits. In dit plan staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan 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 strategisch informatiebeveiligingsbeleid geldt voor alle processen van de Drechtsteden en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de Drechtsteden op het gebied van informatieveiligheid

De organisaties binnen de Drechtsteden hebben een gezamenlijke ambitie en visie voor informatiebeveiliging. *'Wij werken duurzaam veilig, nu en in de toekomst zodat innovatie helpt onze doelen te realiseren".* Deze visie ligt ter grondslag aan dit strategisch informatiebeveiligingsbeleid.

[1] Staatscourant 19 april 2019
[2] BALV (Buitengewone Algemene LedenVergadering) 30 november 2018 (zie ook paragraaf 2.2.2)

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid Drechtsteden voor de jaren "2020 tot 2024". De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

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 deze BIO is meer gericht op risicomanagement dan het oude nomenkader, de BIG. 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. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt.

De principes zijn als volgt:

1. Bestuurders bevorderen 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 (gemeentelijke) organisatie. Deze principes ondersteunen de bestuurder 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 binnen de Drechtsteden

Vanuit de organisaties zijn er binnen de Drechtsteden 10 resultaatgebieden gedefinieerd. Deze resultaatgebieden bieden de organisaties de mogelijkheid om op invoering van de verplichte en gekozen maatregelen te sturen.

De resultaatgebieden zijn:

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 & 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 CISO en de informatiebeveiligingsadviseurs plaats moeten gaan vinden op zowel strategisch als 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 naar 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 dagdagelijkse werkzaamheden.

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 transitieplan en de sourcing strategie wordt het essentieel om op strategisch niveau contacten te hebben en onderhouden met de belangrijke leveranciers om te zorgen dat ook naar de toekomst toe de informatiebeveiliging kan worden geborgd.

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

Incidenten / Crisis management
Indien grote incidenten zich 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 op 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 Drechtstedenorganisaties kennen naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van alle overheden bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[3] 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 op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven Informatiebeveiligingsplan.

2.5 Scope informatiebeveiliging
De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de organisatie en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

[3] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

Dit strategisch regionale Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit (nieuwe) wetgeving af[4]. Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen Deze worden in aanvullende documenten geformuleerd[5].
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt 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 strategische informatiebeveiligingsbeleid. De procesverantwoordelijke maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de organisatie heeft, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet de procesverantwoordelijke dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie. Dit 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 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 burgers en medewerkers.
11. Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

[4] Wetten waaruit aanvullende eisen worden gesteld zijn o.a. AVG, BRP, PNIK, SUWI, BAG, BGT, BRO, DigiD
[5] Lokale handboeken zijn aanvullend op het regionaal beleid. De daarin genoemde aanvullende beveiligingseisen zijn leidend.

- 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 gebruikt worden door de Drechtsteden 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, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening 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 college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is 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 de procesverantwoordelijken adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (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 n.a.v. 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 waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) 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.
- Procesverantwoordelijken dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Procesverantwoordelijken voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

Voor de invulling van de uitgangspunten wordt ook verwezen naar de lokale addendum die is toegevoegd.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

Contractbeheer
De informatiebeveiliging maakt deel uit van afspraken met ketenpartners. In verwerkersovereenkomsten 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 wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
- de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- het dreigingsbeeld gemeenten van de IBD;
- een gezamenlijke risico management sessie georganiseerd door CISO met input van informatiebeveiligingsadviseurs.
- De door de procesverantwoordelijke 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 & 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) 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: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een procesverantwoordelijken. 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. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de organisatie. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de Drechtsteden gezien als een integraal onderdeel van risicomanagement.

Gemeente
De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

3.2 Uitvoering: procesverantwoordelijke

Informatiebeveiliging valt onder de verantwoordelijkheden van alle procesverantwoordelijken. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data en applicaties altijd 1 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 bedrijfsvoeringsoverleg.

Taken van de procesverantwoordelijke 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.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld onder andere door het uitvoeren van quickscans.
- Bespreken van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

Dit Strategisch informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de Gemeente Sliedrecht. De bestuurders en directie van de gemeente Sliedrecht zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.3.1 Zelfevaluatie (ENSIA) en Audit

De organisatie verantwoordt zich over informatiebeveiliging middels de landelijk beschikbaar gestelde zelfevaluatie tool. Voor deze zelfevaluatie en het daaropvolgend audit proces wordt een coördinator aangewezen. 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 verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking. Met deze verklaring van het College van B&W geeft het gemeentebestuur aan in hoeverre de organisatie voldoet aan de afspraken die gemaakt zijn voor de verantwoording Informatiebeveiliging. Eventuele verbetermaatregelen worden hierin meegenomen.

De ingevulde zelfevaluatievragenlijst vormt voor de gemeentelijke organisaties de basis voor het opstellen van de collegeverklaring voor zowel de horizontale als verticale verantwoording.
De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Sliedrecht informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie adequaat te beschermen.

Vastgesteld door het College van B&W van de gemeente Sliedrecht op d.d. ……