Nota voor Burgemeester en Wethouders

Team: Concernstaf
Onderwerp:
Informatiebeveiligingsbeleid 2024

Notagegevens		
Bestuursorgaan	:	B-en-W 16-04-2024
Notanummer	:	2024-302
Datum	:	16-04-2024
Programma	:	11 - Bedrijfsvoering
Portefeuillehouder	:	Burgemeester,
Bijlage(n)	:	Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2024.pdf

Parafering

09-04-2024: Chief information officer
10-04-2024: Burgemeester
09-04-2024: Wethouder

Agendering

* 12-04-2024: Teammanager Concernstaf en Adjunct-secretaris
* 10-04-2024: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

16-04-2024

B & W d.d.: 16-04-2024

Besluit

1. Het informatiebeveiligingsbeleid 2024 vast te stellen
2. De raadsmededeling vast te stellen en aan te bieden aan de gemeenteraad

De nota en het besluit openbaar te maken

Inleiding

Met het geactualiseerde informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende richtinggevende en kaderende stap voor de komende jaren om de beveiliging van persoonsgegevens en andere gemeentelijke informatie te continueren en voort te bouwen op de stappen die in de voorgaande jaren door de DOWR-gemeenten gezet zijn op het gebied van informatieveiligheid en privacy.

Deze beleidsvernieuwing omvat tevens de voorbereiding op de implementatie van belangrijke nieuwe wet- en regelgeving, waaronder de Network and Information Systems Directive (NIS2) en daaruit voortkomend de BIO 2.0 norm die naar verwachting eind 2024 wettelijk verankerd zal worden. Hoewel de BIO 2.0 nog niet definitief is vastgesteld, nemen we reeds stappen om ons voor te bereiden op de verwachte aankomende veranderingen. Dit onderstreept onze proactieve benadering en ons streven naar een tijdige en effectieve naleving van de nieuwe regelgeving.

In overeenstemming met de Informatiebeveiligingsdienst gemeenten (IBD) en de VNG wordt de werkwijze gehanteerd dat het strategisch beleid bestuurlijk door de drie gemeenten moet worden goedgekeurd. Alle onderliggende (tactische/operationele) beleidsstukken zijn in lijn met dit strategisch beleid én de BIO waardoor volstaat om goedkeuring te verkrijgen. De 14 tactische

beleidstukken zijn vastgesteld door de directie.

Het management DOWR-I heeft alle beleidsstukken individueel beoordeeld en akkoord bevonden. Daarnaast is het ook, ter informatie en om duiding te geven, aan de regiegroep, het CIO overleg, directieberaad DOWR en de directie voorgelegd. Hier zijn ook geen bezwaren opgetekend.

Beoogd maatschappelijk resultaat

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Met de vaststelling van het beleid voldoen we aan dit kader.

Kader

* Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2024
* Baseline Informatiebeveiliging Overheden (BIO 2.0): in 2024 van kracht
* i-Visie najaar 2022

Betrokken partijen en participatie

Samenwerkende DOWR-gemeenten.

Toelichting op participatiebeleid

Argumenten voor en tegen

Voor:

1.1 De ontwikkelingen op het gebied van informatieveiligheid gaan snel wat de noodzaak geeft tot actualisatie van het informatiebeveiligingsbeleid

Als er een terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst, is dat digitale veiligheid. Digitale veiligheid vraagt om een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, het voldoen aan wet- en regelgeving, en digitale dreigingen in balans te krijgen en te houden.

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten wijst op een toenemende dreiging, wat wordt bevestigd door voorbeelden van cyberaanvallen op gemeentelijke organisaties in de afgelopen jaren. Het laat zien dat ransomware-aanvallen frequenter voorkomen en ernstigere gevolgen hebben, zoals verstoring van dienstverlening. Bovendien vertoont software meer kwetsbaarheden, waarop we proactief moeten reageren. In lijn hiermee is het essentieel dat we controle blijven uitoefenen over de ketens van onze dienstverlening. Hierbij valt te denken aan de contracten die we afsluiten, de gestelde eisen en de informatie die we delen met leveranciers.

Belangrijke veranderingen ten opzichte van voorgaande jaren zijn:

* Geoblocking:

Dit is een maatregel die ervoor zorgt dat onze digitale systemen niet toegankelijk zijn vanuit landen die bekend staan om hun actieve

cyberoffensieven. Dit betekent dat we de toegang tot onze digitale diensten beperken voor locaties waarvan we weten dat ze een verhoogd risico vormen voor cyberaanvallen. Hierdoor kunnen we de veiligheid van onze systemen versterken en de kans op potentiële bedreigingen verminderen.

* Contractbeheer:

We hebben ons contractbeheer versterkt door beveiligingseisen op te nemen in de contracten met informatieverwerkende leveranciers. Deze eisen zorgen ook ervoor dat leveranciers de gemeente op de hoogte stellen van mogelijke risico's.

* Wachtwoorden:

Het wachtwoordbeleid is vernieuwt vanwege nieuwe technologieën en mogelijkheden. Dit is gedaan om de algehele beveiliging te verbeteren. Tegelijkertijd is er ook aandacht besteed aan het gebruiksvriendelijkheid. Deze veranderingen zijn bedoeld om een betere balans te creëren tussen verbeterde beveiliging en een meer gebruiksvriendelijke ervaring voor de gebruikers.

* Nieuwe werkplek:

Het beleid voor telewerken is aangepast naar een nieuw werkplekconcept met meer flexibiliteit, waarbij gebruik wordt gemaakt van laptopwerkplekken. Dit bevordert een modernere en efficiëntere werkomgeving voor onze medewerkers.

Ook sluiten we met dit beleid aan op de nieuwe i-Visie. Deze aansluiting is minstens zo belangrijk om actief bij te dragen aan de bredere strategische visie op het gebied van digitalisering van onze gemeenten.

Tegen:

Onvoldoende capaciteit en budget voor toekomstige uitvoering.

Financiële consequenties en dekking

Er wordt momenteel een inschatting gemaakt van de verwachte toename in kosten als gevolg van de nieuwe wetgeving. Op dit moment is het huidige budget toereikend, maar we anticiperen op een stijging vanaf 2025.

Op dit moment is de CISO begroot op 0,5 FTE voor de drie organisaties, wat blijkt onvoldoende te zijn, zeker gezien de invoering van de nieuwe wetgeving. Voorbereidingen worden getroffen om een verzoek in te dienen voor een uitbreiding naar 1,0 FTE. Dit zal in de voorjaarsnota worden opgenomen.

Openbaarmaking en communicatie

Nadere communicatie naar aanleiding van dit besluit is niet noodzakelijk.

Aanpak en uitvoering

Na vaststelling van het college van het strategisch informatiebeveiligingsbeleid (bijlage 1) is het informatiebeveiligingsbeleid van kracht.

RAADSMEDEDELING

Onderwerp	Informatiebeveiligingsbeleid 2024		
Nummer	2024-302	**Portefeuillehouder**	Burgemeester,
Team	DEV-CS	**Datum**	16-04-2024

Inleiding
Met het geactualiseerde informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende richtinggevende en kaderende stap voor de komende jaren om de beveiliging van persoonsgegevens en andere gemeentelijke informatie te continueren en voort te bouwen op de stappen die in de voorgaande jaren door de DOWR-gemeenten gezet zijn op het gebied van informatieveiligheid en privacy.

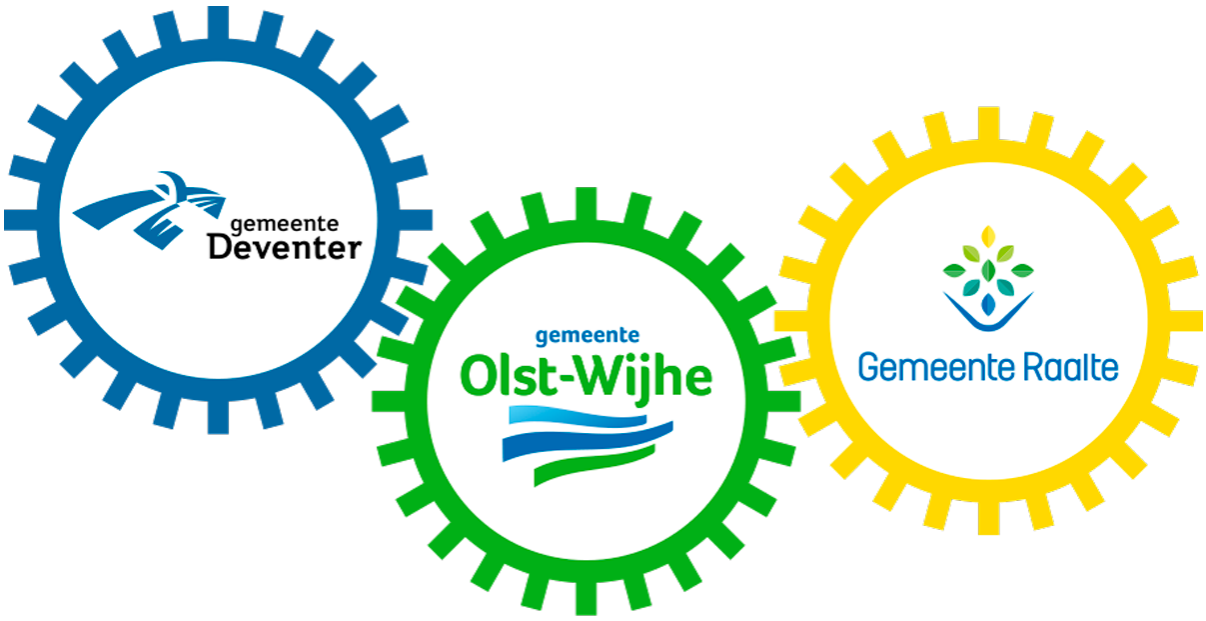
Kader
* Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2024
* Baseline Informatiebeveiliging Overheden (BIO 2.0): in 2024 van kracht
* i-Visie najaar 2022

Kern van de boodschap
Deze beleidsvernieuwing omvat tevens de voorbereiding op de implementatie van belangrijke nieuwe wet- en regelgeving, waaronder de Network and Information Systems Directive (NIS2) en daaruit voortkomend de BIO 2.0 norm die naar verwachting eind 2024 wettelijk verankerd zal worden. Hoewel de BIO 2.0 nog niet definitief is vastgesteld, nemen we reeds stappen om ons voor te bereiden op de verwachte aankomende veranderingen. Dit onderstreept onze proactieve benadering en ons streven naar een tijdige en effectieve naleving van de nieuwe regelgeving.

Nadere toelichting
Als er een terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst, is dat digitale veiligheid. Digitale veiligheid vraagt om een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, het voldoen aan wet- en regelgeving, en digitale dreigingen in balans te krijgen en te houden.

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten wijst op een toenemende dreiging, wat wordt bevestigd door voorbeelden van cyberaanvallen op gemeentelijke organisaties in de afgelopen jaren. Het laat zien dat ransomware-aanvallen frequenter voorkomen en ernstigere gevolgen hebben, zoals verstoring van dienstverlening. Bovendien vertoont software meer kwetsbaarheden, waarop we proactief moeten reageren. In lijn hiermee is het essentieel dat we controle blijven uitoefenen over de ketens van onze dienstverlening. Hierbij valt te denken aan de contracten die we afsluiten, de gestelde eisen en de informatie die we delen met leveranciers.

Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2024



Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Versie:	2.5
Versiedatum:	1 november 2023
Status:	Ter goedkeuring

Versiehistorie

Versie	Datum	Auteur	Rol	Wijziging
1.0	april 2019			Eerste versie naar IBD template
1.1	juni 2019			Actualisatie naar DOWR
1.2	juli 2019			Aansluiting op tactisch en operationeel beleid
1.3	juli 2019			Uitwerking in maatregelen
1.4	augustus 2019			Aansluiting op Beleidskader Informatieveiligheid 2017-2020
1.5	september 2019			Aansluiting op i-Visie 2018-2022
1.6	september 2019			Vermelding onderwerpspecifieke beleidsdocumenten op tactisch en operationeel niveau
1.7	oktober 2019			Versie ter review door team-manager DOWR I-werkorganisatie
1.9	oktober 2019			Laatste versie voor review door inhoudsdeskundigen
2.0	oktober 2019			Versie ter goedkeuring
2.1	september 2023			Aansluiting op BIO 2.0-opmaat
2.2	september 2023			Aansluiting op i-Visie najaar 2022
2.3	oktober 2023			Aansluiting op Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023-2024
2.4	oktober 2023			Laatste versie voor review door inhoudsdeskundigen
2.5	november 2023			Versie ter goedkeuring

Goedkeuringsproces

Versie	Datum	Functionaris / Orgaan	Status
2.5	1 november 2023		Goedkeuring namens team Informatiebeveiliging DOWR
2.5	3 november 2023	Managementteam DOWR-I	Goedkeuring namens management DOWR-I
2.5	8 november 2023	I-Regiegroep DOWR	Instemming namens I-Regiegroep DOWR
2.5	5 december 2023	CIO-overleg DOWR	Instemming namens Chief Information Officers DOWR
2.5	1 februari 2024	Directieberaad DOWR	Instemming namens directieberaad DOWR
2.5	13 maart 2024	Directie Deventer	Instemming namens directie gemeente Deventer
2.5	13 maart 2024	Directie Olst-Wijhe	Instemming namens directie gemeente Olst-Wijhe
2.5		Directie Raalte	Instemming namens directie gemeente Raalte
2.5		College van B&W Deventer	Vaststelling door B&W gemeente Deventer
2.5		College van B&W Olst-Wijhe	Vaststelling door B&W gemeente Olst-Wijhe
2.5		College van B&W Raalte	Vaststelling door B&W gemeente Raalte

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Inhoudsopgave

1 Inleiding

Als er een terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst is dat digitale veiligheid. Digitale veiligheid vraagt om een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, het voldoen aan wet- en regelgeving en digitale dreigingen in balans te krijgen en te houden.
Een belangrijke verandering die de digitale weerbaarheid kan vergroten is de vernieuwing van Europese wet- en regelgeving die van toepassing wordt op de lokale overheid. Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten laat zien dat de dreiging toeneemt, wat onderschreven wordt door de voorbeelden van cyberaanvallen op gemeentelijke organisaties de afgelopen jaren.

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid van de DOWR-gemeenten vanaf het jaar 2024, houdt in afgeleide rekening met voorgenoemde ontwikkelingen en vervangt het in 2020 vastgestelde Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch en operationeel niveau.

Het voorliggende strategisch informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), het normenkader voor alle gemeenten en gemeentelijke samenwerkingsverbanden. Hoewel op het moment van schrijven BIO 1.04 nog de geldende norm is, zijn de voorgestelde wijzigingen voor de toekomstige BIO 2.0 (geactualiseerd naar de ISO 27002:2022 norm) reeds in dit beleid verwerkt. De aangepaste maatregelen zijn gebaseerd op de in juli 2023 verschenen handreiking ‘BIO 2.0-opmaat’. De implementatie van BIO 2.0 staat gepland voor het najaar van 2024 inclusief wettelijke verankering in de Wbni (Wet beveiliging netwerk- en informatiesystemen).

Met dit strategisch informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende richtinggevende en kaderende stap voor de komende jaren om de beveiliging van persoonsgegevens en andere gemeentelijke informatie te continueren en voort te bouwen op de stappen die in de voorgaande jaren door de DOWR-gemeenten gezet zijn op het gebied van informatieveiligheid en privacy.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch informatiebeveiligingsbeleid uiteengezet. Dit strategisch beleid wordt aangevuld met onderwerpspecifieke beleidsdocumenten die dit beleid op tactisch en operationeel niveau concretiseren. Onder leiding van de Chief Information Security Officer (CISO) wordt ieder jaar een gemeentelijk Informatiebeveiligingsplan (IBP) opgesteld en vastgesteld door de directies van de gemeenten Deventer, Olst-Wijhe en Raalte. In het IBP worden de tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt, aangevuld met de planning van concrete acties om de praktijk in overeenstemming te brengen met de maatregelen uit het beleid.
Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging in de organisatie belegd zijn.
Ten slotte wordt in hoofdstuk 4 het strategisch beleid concreet uitgewerkt in maatregelen.

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 informatiebeveiligingsbeleid geldt voor alle gemeentelijke processen 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 onverkort betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

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

De ambitie en visie van de DOWR-gemeenten op het gebied van de informatievoorziening is uitgewerkt in de in het najaar van 2022 geactualiseerde i-Visie zoals in november 2022 vastgesteld door de colleges van B&W van de gemeenten Deventer, Olst-Wijhe en Raalte.
De thema's uit deze i-Visie die in direct verband staan met informatieveiligheid zijn hieronder opgenomen en toegelicht.

Informatieveiligheid, privacy en ethiek als topprioriteit; stabiliteit als randvoorwaarde

De DOWR-gemeenten geven de hoogste prioriteit aan informatieveiligheid en de bescherming van persoonsgegevens. Voor het verwerken van privacygevoelige informatie wordt de AVG gevolgd. Er wordt een ethisch kader ontwikkeld om de effecten van het inzetten van informatietechnologie op de publieke waarden zorgvuldig af te wegen. De stabiliteit van de DOWR-informatievoorziening is randvoorwaardelijk om de continuïteit van de bedrijfsprocessen te kunnen borgen.

Digitalisering van de bedrijfsvoering

De bedrijfsvoering van de DOWR-gemeenten ondersteunen de gemeentelijke organisaties in de volledige breedte voor het realiseren van hun ambities. Hybride werken is hierbij niet meer weg te denken. Slimme digitale toepassingen en datagedreven werken dragen bij aan het efficiënter uitvoeren van werkzaamheden.

Informatie- en archiefbeheer op orde

De DOWR-gemeenten sturen op kwaliteit en toegankelijkheid van informatie, waardoor transparantie gewaarborgd is en WOO-verzoeken efficiënt beantwoord kunnen worden.

Informatievoorziening in samenwerkingsverbanden

De DOWR-gemeenten opereren veel in samenwerkingsverbanden. Als regieorganisatie blijft de gemeente eindverantwoordelijk voor de dienstverlening aan burgers en bedrijven. De DOWR-gemeenten onderkennen daarom het belang van goede (online) samenwerkingsomgevingen, koppelingen tussen taakapplicaties en eisen aan de interne informatiehuishouding van de verbonden partij, waaronder informatiebeheer, informatieveiligheid, privacy en ethiek.

Besturing en bedrijfsvoering van de informatiehuishouding

Informatievoorziening wordt door de DOWR-gemeenten als strategische factor gezien, en wordt daarom goed verankerd in de domeinen (sociaal, fysiek, publieke dienstverlening en bedrijfsvoering). Bovendien adviseert en ondersteunt DOWR-i op het gebied van informatievoorziening en stuurt het op informatieveiligheid en stabiliteit.

Betrouwbare en open overheid

De DOWR-gemeenten willen betrouwbare en open gemeenten zijn: gemeenten die actief informatie delen met de samenleving. Hierbij worden de landelijke richtlijnen en wetgeving gevolgd, met als doel de overheid transparanter te maken met inachtneming van de bescherming van de privacy van inwoners en ondernemers.

2 Strategisch beleid

Het doel van deze beleidsnota is het presenteren van het strategisch informatiebeveiligingsbeleid van de DOWR-gemeenten vanaf het jaar 2024.

2.1 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid worden hieronder toegelicht.

BIO 2.0, ISO 27001/27002, NIS2 en Wbni

Sinds 1 januari 2020 geldt de BIO (Baseline Informatiebeveiliging Overheid) als het normenkader voor informatiebeveiliging binnen de overheid. Het beveiligingsbeleid is gebaseerd op de ISO 27001 standaard, terwijl de ISO 27002 norm (aangevuld met overheidsmaatregelen) dient als basis voor de controls in de BIO norm. Oorspronkelijk was een evaluatie van de BIO norm gepland voor 2023, maar vanwege de introductie van de ISO 27002:2022 norm is dit vervroegd naar 2022.

Er is ook een belangrijke ontwikkeling op het gebied van Europese richtlijnen, namelijk de herziening van de Network and Information Security (NIS) richtlijn[1]. De nieuwe NIS2 richtlijn is op 28 november 2022 door de Europese Raad vastgesteld en is ook van toepassing op de lokale overheid. Deze richtlijn wordt omgezet naar Nederlandse wetgeving als onderdeel van de herziening van de Wet beveiliging netwerk- en informatiesystemen (Wbni), gepland voor het najaar van 2024[2].

BIO 2.0 zal het nieuwe normenkader vormen voor informatiebeveiliging binnen de overheid. Hierin zijn zowel de ISO 27002:2022 norm als de NIS2 richtlijn verwerkt, met wettelijke verankering in de Wbni. In juli 2023 is een voorlopige versie van BIO 2.0 uitgebracht in de vorm van de handreiking 'BIO 2.0-opmaat'. De wijzigingen in deze handreiking zijn opgenomen in het voorliggende strategische informatiebeveiligingsbeleid en de onderliggende beleidsdocumenten voor informatiebeveiliging op tactisch en operationeel niveau.

Het is echter niet uit te sluiten dat er nog aanvullende eisen en/of maatregelen uit de NIS2 richtlijn worden toegevoegd aan de uiteindelijke versie van BIO 2.0. Als deze wijzigingen gevolgen hebben voor het informatiebeveiligingsbeleid van de DOWR-gemeenten, dan worden de desbetreffende documenten herzien en opnieuw ter goedkeuring en vaststelling aangeboden.

Risicomanagement

De BIO norm richt zich vooral op het toepassen van risicomanagement. Met behulp van een risico-afweging wordt een inschatting gemaakt van de mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van de mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

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 op het gebied van beschik-baarheid, integriteit en vertrouwelijkheid.

[1] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn
[2] https://www.bio-overheid.nl/uitgelicht

De 10 principes voor informatiebeveiliging

In 2019 heeft de VNG 10 principes voor informatiebeveiliging[3] opgesteld. Deze zijn een bestuurlijke aanvulling op de 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 en ondersteunen de bestuurder bij het uitvoeren van goed risico-management. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[4], opgesteld door de Informatie-beveiligingsdienst (IBD), geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld heeft als doel gemeenten weerbaarder te maken op het gebied van informatiebeveiliging en is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen op dit gebied.

Informatie uit incidenten

De DOWR-gemeenten kennen ten slotte ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren. Daarom worden evaluaties van incidenten uit het verleden ook nadrukkelijk gebruikt bij het actualiseren van het beleid.

[3] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[4] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024

2.2 Plaats van het strategisch beleid

Het strategisch informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven aan de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De vertaling naar tactische en operationele richtlijnen en maatregelen is geconcretiseerd in de volgende onderwerpspecifieke beleidsdocumenten:

- Beleid Anti-Malware DOWR-gemeenten
- Beleid Backup en Recovery DOWR-gemeenten
- Beleid Change Management DOWR-gemeenten
- Beleid Cloud Computing DOWR-gemeenten
- Beleid Contract Management DOWR-gemeenten
- Beleid Encryptie DOWR-gemeenten
- Beleid Fysieke Beveiliging DOWR-gemeenten
- Beleid Incident Management en Response DOWR-gemeenten
- Beleid Logging en Monitoring DOWR-gemeenten
- Beleid Logische Toegangsbeveiliging DOWR-gemeenten
- Beleid Mobiele Apparaten DOWR-gemeenten
- Beleid Personeel DOWR-gemeenten
- Beleid Telewerken DOWR-gemeenten
- Beleid Wachtwoorden DOWR-gemeenten

De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Informatiebeveiligingsplan (IBP), aangevuld met de planning van concrete acties om de praktijk in overeenstemming te brengen met de maatregelen uit het beleid.

2.3 Scope

De scope van het informatiebeveiligingsbeleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente (ook als deze bij externe leveranciers en ketenpartners is ondergebracht), evenals het gebruik daarvan door medewerkers en ingehuurd personeel in de meest brede zin van het woord.

Dit strategisch informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af, bijvoorbeeld vanuit BRP[5], SUWI[6] en AVG[7].

2.4 Uitgangspunten

Het bestuur, de directie en het middenmanagement (zijnde de teammanagers, teamleiders, domein-managers en programmamanagers van de gemeenten Deventer, Olst-Wijhe en Raalte) spelen een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid door het belang van de verschillende delen van de informatievoorziening in te schatten, de risico's in beeld te brengen en te bepalen welke van deze risico's onacceptabel hoog zijn.
Voor een nauwkeurige inschatting van de risico's wordt van het middenmanagement nadrukkelijk afstemming met het hoger management verlangd. Dit is essentieel om de impact op gerelateerde processen juist te kunnen beoordelen. Risico's met potentiële impact op de gehele organisatie moeten beoordeeld worden op directieniveau.

[5] De Basisregistratie Personen (BRP) bevat persoonsgegevens van inwoners van Nederland (ingezetenen) en personen die Nederland hebben verlaten (niet ingezetenen).
[6] In de wet SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) is geregeld hoe de werknemersverzekeringen en de volksverzekeringen worden uitgevoerd.
[7] De Algemene Verordening Gegevensbescherming (AVG) is een Europese verordening die de regels voor de verwerking van persoonsgegevens door bedrijven en overheidsinstanties in de Europese Unie standaardiseert.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van het informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeenten Deventer, Olst-Wijhe en Raalte en de relevante landelijke en Europese wet- en regelgeving.

Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- De DOWR-gemeenten staan garant voor correcte en veilige informatievoorzieningen.
- De DOWR-gemeenten zijn weerbaar tegen cyberaanvallen en beschermen haar vitale belangen in het cyberdomein.
- De DOWR-gemeenten handelen op het gebied van informatiebeveiliging in lijn met het algemene beleid en de relevante landelijke Europese wet- en regelgeving.
- De DOWR-gemeenten beschikken over voldoende kennis en kunde op het gebied van cybersecurity en investeren in ICT-innovatie om haar doelstellingen op het gebied van informatieveiligheid en privacy te behalen.
- De DOWR-gemeenten bouwen aan coalities met overheidspartners binnen het cyberdomein.
- De DOWR-gemeenten investeren in veilige en betrouwbare ICT-producten en -diensten ter bescherming van de informatie en de privacy van haar medewerkers, burgers en bedrijven.

Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het strategisch informatiebeveiligingsbeleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente. Bepaalde informatie is zelfs van vitaal belang. Het college van B&W is eindverantwoordelijk voor de beveiliging van alle gemeentelijke informatie.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiesystemen die gebruikt worden door de gemeente hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming daarvan 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 Informatiebeveiligingsplan (IBP) het fundament onder een betrouwbare informatievoorziening. In het IBP wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. De fasen Plan, Do, Check en Act (PDCA) vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente 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.
- Iedere medewerker is verplicht om gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.5 Randvoorwaarden

De belangrijkste randvoorwaarden voor het strategisch informatiebeveiligingsbeleid zijn:

- Externe leveranciers en ketenpartners buiten de overheid zijn zelf niet rechtstreeks gebonden aan de BIO, maar moeten wel voldoen aan de eisen van de opdrachtgever. Alle voorwaarden om te voldoen aan het informatiebeveiligingsbeleid van de gemeente moeten daarom in de contracten zijn vastgelegd.
- Kennis en bewustzijn van informatiebeveiliging en het omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een Informatiebeveiligingsplan (IBP) opgesteld onder leiding van de CISO. Hierin worden de tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt, aangevuld met de planning van concrete acties om de praktijk in overeenstemming te brengen met de maatregelen uit het beleid. Het IBP is gebaseerd op de volgende bronnen:
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA)[8].
    - Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, opgesteld door de Informatiebeveiligingsdienst (IBD).
    - De door de teammanagers, teamleiders, domeinmanagers en programmamanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

[8] ENSIA (Eenduidige Normatiek Single Information Audit) heeft als doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke P&C-cyclus.

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 Defense (3LoD). In dit model is het lijnmanagement als eerste lijn verantwoordelijk voor de eigen processen. De tweede lijn (de CISO en de Security Officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door (interne of externe) auditors van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directieteam

De directies van de gemeenten Deventer, Olst-Wijhe en Raalte zorgen dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager, teamleider, domeinmanager of programmamanager. De directie zorgt dat zij zich verantwoorden over de beveiliging van de onder hen ressorterende informatie. 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.

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. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: middenmanagement

Informatiebeveiliging valt onder de verantwoordelijkheden van de teammanagers, teamleiders, domeinmanagers en programmamanagers. 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 minimaal één eigenaar hebben. Er moet dus altijd iemand verantwoordelijk zijn. Teammanagers, teamleiders, domeinmanagers en programmamanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van het middenmanagement in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Escalatie naar directieniveau voor de beoordeling van risico's met potentiële impact op de gehele organisatie.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

De voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het gemeentebestuur van Deventer, Olst-Wijhe en Raalte. Het bestuur en de directie van de gemeente 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 de respectievelijke portefeuille-houders. Daarnaast rapporteert de directie over de mate waarin zij invulling geeft aan het uitwerken van tactische beleidsonderwerpen die aanvullend zijn op dit strategisch beleid.

ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek.
ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatie-verstrekking en eenmalige IT-audit.
ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. De focus ligt hierbij op de horizontale verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. ENSIA is een initiatief van de VNG en de ministeries van BZK, I&W en SZW.

ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid, gebaseerd op de BIO. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de P&C-cyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid, over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).

De gemeentesecretaris wijst de ENSIA-coördinator aan, die ervoor zorgt dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers, teamleiders, domeinmanagers en programmamanagers. Zij leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de Collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de college-verklaring aan de raad.

Middels deze verantwoording worden het gemeentebestuur en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Auditplan

Jaarlijks wordt door de ENSIA-coördinator een auditplan opgesteld en door de CISO vastgesteld. Dit auditplan beschrijft het auditproces en voor welke processen en informatiesystemen een audit uitgevoerd wordt. Deze kunnen door interne of externe auditors, of (in geval van technische audits) geautomatiseerd worden uitgevoerd. Audits en kwetsbaarheidsanalyses dienen een objectief oordeel te geven. In de rapportages worden ook de mogelijkheden tot verbetering uitgewerkt.

ISMS

Door periodieke controle, organisatiebrede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Om het doorlopende verbeterproces van informatiebeveiliging op gestructureerde wijze te borgen, is er een Information Security Management System (ISMS) ingericht waarin de gehele PDCA-cyclus (Plan, Do, Check, Act) aantoonbaar wordt vastgelegd. Deze cyclus houdt het volgende in:

- Regels en uitgangspunten zijn opgesteld ten aanzien van informatieveiligheid (in de vorm van het informatiebeveiligingsbeleid).
- Kwetsbaarheden zijn geanalyseerd en verbeterpunten zijn geïdentificeerd (in de vorm van risicoanalyses).
- Een verbeterplan is opgesteld (in de vorm van het Informatiebeveiligingsplan, aangevuld met de planning van concrete acties).
- Er wordt gemonitord op de kwaliteit en de uitvoering van het verbeterplan.

Als er aan de bovenstaande elementen wordt voldaan, is er sprake van een sluitend ISMS. Met het ISMS wordt dus niet gedoeld op een softwaretool, maar op een continu verbeterproces waarmee de informatieveiligheid wordt gewaarborgd.

4 Uitwerking in maatregelen

Het strategisch informatiebeveiligingsbeleid is concreet uitgewerkt in de hieronder weergegeven maatregelen.

Vaststelling van het beleid

1. Het college van B&W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
2. Zowel het strategisch informatiebeveiligingsbeleid als de onderwerpspecifieke beleids-documenten worden minimaal één keer per 3 jaar, evenals bij significante veranderingen, opnieuw beoordeeld en zo nodig bijgesteld, goedgekeurd door de directie, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden.
3. De directie stelt jaarlijks het Informatiebeveiligingsplan (IBP) vast, waarin het informatie-beveiligingsbeleid in concrete maatregelen is uitgewerkt.
4. De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op het strategisch informatiebeveiligingsbeleid.

Uitvoering van de maatregelen

5. De teammanagers, teamleiders, domeinmanagers en programmamanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn. Zij zijn de proceseigenaren.
6. De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. De proces-eigenaren voeren de Baselinetoets BIO uit om deze risicoafwegingen te kunnen maken.
7. Om het doorlopende verbeterproces van informatiebeveiliging op gestructureerde wijze te borgen, is er een Information Security Management System (ISMS) ingericht waarin de gehele PDCA-cyclus (Plan, Do, Check, Act) aantoonbaar wordt vastgelegd.

Controle op naleving van het beleid

8. De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers, teamleiders, domeinmanagers en programmamanagers, en ziet erop toe dat zij adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
9. De teammanagers, teamleiders, domeinmanagers en programmamanagers 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.

Rol en verantwoordelijkheid van de CISO

10. Er is een Chief Information Security Officer (CISO) aangesteld conform een vastgesteld CISO-functieprofiel waarin de rol en verantwoordelijkheden zijn vastgelegd.
11. De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de veiligheid en betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
12. 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.
13. De CISO stelt jaarlijks het door de ENSIA-coördinator opgestelde auditplan vast, waarin wordt bepaald voor welke processen en informatiesystemen een audit uitgevoerd wordt.

Rol en verantwoordelijkheid van de FG

14. Er is een Functionaris Gegevensbescherming (FG) aangesteld conform een vastgesteld FG-functieprofiel waarin de rol en verantwoordelijkheden zijn vastgelegd.
15. De FG controleert regelmatig de naleving van de privacyregels conform de AVG en het beveiligingsbeleid van de gemeente.

Audits en kwetsbaarheidsanalyses

16. Conform het auditplan (vastgesteld door de CISO) worden jaarlijks audits uitgevoerd op geselecteerde processen en informatiesystemen.
17. Informatiesystemen worden periodiek gecontroleerd op de technische naleving van beveiligingsnormen en risico's op het gebied van informatieveiligheid. Dit kan door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten.
18. Audits en kwetsbaarheidsanalyses dienen objectief te beoordelen of aan de wet- en regelgeving en het beveiligingsbeleid van de gemeente voldaan wordt.
19. In rapportages naar aanleiding van audits en kwetsbaarheidsanalyses worden ook de mogelijkheden tot verbetering uitgewerkt.

Training van medewerkers

20. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
21. Medewerkers dienen verantwoord om te gaan met vertrouwelijke informatie (waaronder persoonsgegevens).

Contact met instanties en toezichthouders

22. De gemeente onderhoudt passende contacten met relevante instanties en toezichthouders.
23. Er is een overzicht van instanties en toezichthouders waar de gemeente contacten mee onderhoudt, met welk doel de contacten ingezet worden en welke eisen relevant zijn.
24. Het contactoverzicht met instanties en toezichthouders wordt jaarlijks geactualiseerd.