Nota voor Burgemeester en Wethouders

Team: Concernstaf
Onderwerp:
Strategisch informatiebeveiligingsbeleid DOWR

Notagegevens		
Bestuursorgaan	:	B-en-W 13-12-2022
Notanummer	:	2022-1077
Datum	:	13-12-2022
Programma	:	11 - Bedrijfsvoering
Portefeuillehouder	:	Burgemeester,
Bijlage(n)	:	Addendum verlenging IB beleid DOWR 2023.pdf,Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022.pdf

Parafering

07-12-2022: Programmamanager
30-11-2022: Burgemeester

Agendering

* 08-12-2022: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

B & W d.d.: 13-12-2022

Besluit

1. De geldigheidsduur van het ‘Strategische Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022’ met één jaar te verlengen
2. Het addendum vast te stellen t.b.v. verlenging IB beleid DOWR 2023 als oplegger bij aanpalend beleid

Inleiding

Het Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022 loopt eind 2022 af en dient formeel in 2022 vernieuwd te worden vastgesteld. In 2023 wordt echter de nieuwe wettelijke Baseline Informatiebeveiliging Overheden (BIO 2.0) van kracht. Deze nieuwe baseline vormt een belangrijke basis voor herziening van het informatiebeveiligingsbeleid voor de DOWR-gemeenten. Wachten met herziening tot in 2023 en verlenging van het geldende informatiebeveiligingsbeleid van DOWR ligt daarom voor de hand.

Beoogd maatschappelijk resultaat

Een eenduidig kader in de drie DOWR-gemeenten voor informatiebeveiliging.

Kader

* Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022
* Baseline Informatiebeveiliging Overheden (BIO 2.0): in 2023 van kracht

Betrokken partijen en participatie
Samenwerkende DOWR-gemeenten.

Argumenten voor en tegen
1. Het huidige informatiebeveiligingsbeleid is nog steeds actueel en passend;
2. Het nieuwe normenkader (BIO 2) verschijnt in 2023 en vormt een belangrijke basis voor herziening van het informatiebeveiligingsbeleid.

Financiële consequenties en dekking
Kosten zijn gedekt conform de reguliere begroting van DOWR-i.

Openbaarmaking en communicatie
Nadere communicatie naar aanleiding van dit besluit is niet nodig.

Aanpak en uitvoering
In 2023 volgt herziening van het informatiebeveiligingsbeleid.

Addendum

Onderwerp
Verlenging geldigheidsduur informatiebeveiligingsbeleid

Aanleiding
Eind 2022 is door de individuele colleges van de gemeenten Deventer, Olst-Wijhe en Raalte (DOWR) besloten dat het Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022 met een jaar wordt verlengd tot uiterlijk 1-1-2024.
Aanleiding hiervoor is de komst van de nieuwe Baseline Informatiebeveiliging Overheid (BIO) 2.0 welke op dit moment nog in ontwikkeling is en naar verwachting in 2023 vastgesteld zal worden. Dit nieuwe BIO-normenkader zal als basis dienen voor het opnieuw vast te stellen strategisch informatiebeveiligings-beleid en de onderliggende beleidsdocumenten op tactisch en operationeel niveau:

- 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

Collegebesluit
De colleges van de DOWR-gemeenten hebben besloten het Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022 ongewijzigd met een jaar te verlengen tot uiterlijk 1-1-2024.

CISO DOWR-gemeenten

november 2022

Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022

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

Versie:	2.0
Versiedatum:	24 oktober 2019
Status:	Vastgesteld

Versiehistorie

Versie	Datum	Auteur	Rol	Wijziging
1.0	april 2019		TISO	Eerste versie naar IBD template

Goedkeuringsproces

Versie	Datum	Functionaris / Orgaan	Status
2.0	24-10-2019	(CISO a.i.)	Goedkeuring namens team Informatiebeveiliging DOWR

Inhoudsopgave

1 Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot en met 2022 en vervangt het in 2017 vastgestelde Beleidskader Informatieveiligheid 2017-2020.
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. De BIO is per 2020 de opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG) waarbij het jaar 2019 als overgangsjaar is ingesteld. Het grote verschil tussen de BIG en de BIO is dat de BIO op de ISO 27002 norm is gebaseerd en meer ruimte geeft voor het treffen van passende maatregelen op basis van risicomanagement.

Met dit strategisch informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende stap 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 samenwerkende 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 Concern 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 processen van de gemeenten Deventer, Olst-Wijhe en Raalte 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 i-Visie 2018-2022 zoals in november 2017 vastgesteld door de gemeenteraden van 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 en stabiliteit als topprioriteit i-Visie 2018-2022, thema 1

De DOWR-gemeenten geven de hoogste prioriteit aan informatieveiligheid en de bescherming van persoonsgegevens. Daarom worden er aanvullende maatregelen getroffen en serieuze investeringen gedaan om onder andere te voldoen aan de BIO.

Sluitend informatiebeheer i-Visie 2018-2022, thema 2

De DOWR-gemeenten werken toe naar een volledig digitaal archief van gestructureerde en ongestructureerde procesdocumenten. Waar mogelijk wordt aangesloten op de trend van landelijke producten, standaarden en voorzieningen. Hierdoor ontstaat minder behoefte aan lokale oplossingen en daarmee lokaal beheer.

Beleid maken en uitvoeren met open data en open overheid i-Visie 2018-2022, thema 6

De DOWR-gemeenten gaan sets van open data, die landelijk aangewezen zijn, actief ter beschikking stellen, om zo andere publieke en private partijen in staat te stellen om nieuwe diensten te ontwikkelen. Dit wordt gedaan conform landelijke richtlijnen op (landelijke) online voorzieningen.

Informatievoorziening met ketenpartners en verbonden partijen i-Visie 2018-2022, thema 8

De DOWR-gemeenten opereren meer en meer als netwerkorganisaties in veelvormige en veelsoortige, al dan niet geformaliseerde samenwerkingsverbanden. Als regieorganisatie blijft de gemeente eindverantwoordelijk voor de dienstverlening. Het borgen van kennis en toezicht en het op niveau houden van de dienstverlening aan burgers en bedrijven heeft de prioriteit.
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 informatieveiligheid.

Digitalisering van de interne bedrijfsvoering i-Visie 2018-2022, thema 9

De DOWR-gemeenten moderniseren de interne bedrijfsvoering nog verder, met zelfservice voor medewerkers en leidinggevenden, plaats- en tijdonafhankelijke communicatiemiddelen en vergroting van de wendbaarheid door het verminderen van het aantal applicaties. Hierbij wordt de trend richting de cloud gevolgd.

Besturing en bedrijfsvoering van de informatiehuishouding i-Visie 2018-2022, thema 10

De DOWR-gemeenten vinden de informatievoorziening een strategische factor, te benaderen vanuit maatschappelijke opgaven en gemeentelijke doelen. Informatievoorziening en ICT worden bestuurd door middel van de DOWR-brede i-Visie met ruimte voor lokaal beleid. De uitvoering geschiedt programmatisch en de voortgang wordt periodiek verantwoord als integraal onderdeel van de P&C-cyclus.
De DOWR i-werkorganisatie zorgt voor de instandhouding van DOWR-brede informatiesystemen en de 'harde ICT'. Daarnaast adviseert en ondersteunt DOWR-i binnen de kaders en stuurt op informatieveiligheid en stabiliteit.

2 Strategisch beleid

Het doel van deze beleidsnota is het presenteren van het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot en met 2022.

2.1 Ontwikkelingen

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

BIO (Baseline Informatiebeveiliging Overheid)

De BIO is met ingang van 1 januari 2020 het nieuwe normenkader voor informatiebeveiliging voor de overheid. De werkwijze van de BIO is meer gericht op risicomanagement dan de oude BIG (Baseline Informatiebeveiliging Gemeenten).

Met behulp van een risicoafweging 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.

De 10 principes voor informatiebeveiliging

In 2019 heeft de VNG 10 principes voor informatiebeveiliging[1] 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.

[1] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[2], opgesteld door de Informatiebeveiligingsdienst (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.

2.2 Standaarden

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.

Op basis van de bovengenoemde NEN-ISO normen is in 2018 door de interbestuurlijke werkgroep Normatiek[3] de BIO uitgebracht. Ook zijn praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

2.3 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] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2019-2020
[3] De interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld de VNG en de IBD, maar ook waterschappen, provincies en het rijk.

2.4 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[4], SUWI[5] en AVG[6].

2.5 Uitgangspunten

Het bestuur, de directie en het middenmanagement (zijnde de teammanagers, teamleiders en domeinmanagers 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.

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.

[4] De Basisregistratie Personen (BRP) bevat persoonsgegevens van inwoners van Nederland (ingezetenen) en personen die Nederland hebben verlaten (niet ingezetenen).
[5] In de wet SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) is geregeld hoe de werknemersverzekeringen en de volksverzekeringen worden uitgevoerd.
[6] 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.

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.

2.6 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)[7].
    - Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, opgesteld door de Informatiebeveiligingsdienst (IBD).
    - De door de teammanagers, teamleiders en domeinmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

[7] 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 of domeinmanager. 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 en domeinmanagers. 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 en domeinmanagers 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.
- 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 en domeinmanagers. 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 beleid 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. Hierdoor wordt gewaarborgd dat het beleid voortdurend passend, adequaat en doeltreffend is.
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 en domeinmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn. Zij zijn de proces-eigenaren.
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 en domeinmanagers, 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 en domeinmanagers 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 Concern 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. Audits en kwetsbaarheidsanalyses kunnen door interne of externe auditors, of (bij technische audits) geautomatiseerd worden uitgevoerd.
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.