B&W Adviesnota

Onderwerp	Vastelling Informatiebeveiligingsbeleid 2024-2026
Zaaknummer	
B&W datum	17 december 2024
Naam steller	Medewerker team Informatie en Automatisering
Teammanager	Teammanager team Informatie en Automatisering
Portefeuillehouder	Wim de Schryver

Besproken met portefeuillehouder?
Ja, met Wim de Schryver op 16 december 2024
Openbaarheid
Ja, per direct.
Bevoegd orgaan
B en W
N.v.t.

Advies

1. Akkoord te gaan met de verlenging van het huidige informatiebeveiligingsbeleid tot en met 2026.
2. Akkoord te gaan met het Addendum informatiebeveiligingsbeleid 2024-2026

Inleiding

Het huidige informatiebeveiligingsbeleid, geldig tot eind 2023, is verouderd en dient daarom opnieuw te worden vastgesteld. Op 17 oktober is de Europese NIS2[1]-richtlijn in werking getreden. De lidstaten, waaronder Nederland, moesten voor deze datum de richtlijn hebben omgezet in nationale wetgeving, voor Nederland is dat de Cyberbeveiligingswet (Cbw)[2]. Nederland heeft aangegeven deze deadline niet te halen. Naar verwachting zal de Cbw in augustus 2025 in werking treden.

Door de komst van de Cbw wordt ook de Baseline Informatiebeveiliging Overheid (BIO) aangepast naar de BIO2. Deze baseline wordt wettelijk verplicht via de NIS2 implementatie in de Cyberbeveiligingswet.

Gezien de bovenstaande wijzigingen, die naar verwachting in het derde kwartaal van 2025 van kracht worden en de daaruit voortvloeiende nieuwe verplichtingen, is het niet zinvol om voor de korte tussenliggende periode (< 1 jaar) een volledig nieuw informatiebeveiligingsbeleid op te stellen.

Het voorstel is daarom om het huidige informatiebeveiligingsbeleid te verlengen tot en met 2026, zodat de gemeente Venray tot aan de ingangsdatum van de Cbw een geldig informatiebeveiligingsbeleid heeft. Er is gekozen om het beleid een geldigheidsduur te geven tot 2026, zodat bij eventuele vertraging in de inwerkingtreding van de Cbw het beleid in 2026 niet opnieuw hoeft te worden vastgesteld.

[1] Network and Information Security directive: L_2022333NL.01008001.xml (europa.eu)
[2] Cyberbeveiligingswet (NIS2-richtlijn) | Over het NCSC | Nationaal Cyber Security Centrum

Het bij deze nota vast te stellen beleid en het bijbehorende addendum zullen worden vervangen door een nieuw informatiebeveiligingsbeleid zodra de Cbw in werking treedt en de gevolgen daarvan voor het huidige beleid duidelijk zijn.

Beoogd resultaat

Een actueel vastgesteld informatiebeveiligingsbeleid.

Argumenten

1.1 Een actueel informatiebeveiligingsbeleid is een vereiste

Een actueel vastgesteld informatiebeveiligingsbeleid is een vereiste conform de BIO en dient als bewijsstuk voor de diverse jaarlijkse audits.

2.1 Voldoen aan de huidige DigiD normen[3]

Het addendum op het informatiebeveiligingsbeleid 2024-2026 is noodzakelijk om te voldoen aan de norm B.01 van de dit jaar gewijzigde DigiD-normen die ook getoetst wordt op werking.

Kanttekeningen of risico's

1.1 Het niet opnieuw vaststellen van het informatiebeveiligingsbeleid zorgt ervoor dat we wet en regelgeving niet naleven.

1.2 Een verouderd informatiebeveiligingsbeleid kan zorgen voor reputatieschade bij datalekken en beveiligingsincidenten.

2.1 Het niet vaststellen van het addendum zorgt ervoor dat we als organisatie niet voldoen aan de gestelde B.01 norm met betrekking tot DigiD.

Communicatie

Het vastgestelde informatiebeveiligingsbeleid vervangt het informatiebeveiligingsbeleid 2020-2023 op VENnet zodat deze voor iedereen te raadplegen is.

Financiële gevolgen

n.v.t.

Vervolgtraject besluitvorming

n.v.t.

Evaluatie

n.v.t.

Bijlagen

Informatiebeveiligingsbeleid 2024-2026
Addendum informatiebeveiligingsbeleid 2024-2026

[3] Logius | Normenkader 3.0 voor ICT-beveiligingsassessments DigiD

Informatiebeveiligingsbeleid 2024 tot 2026

07-10-2024
J. Frencken
IV

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot 2026 en vervangt het in 2023 vastgestelde 'Informatiebeveiligingsbeleid 2020-2023'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Informatiebeveiligingsbeleid 2024-2026' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de 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 die aanvullend zijn op dit strategisch beleid. In een jaarlijks uit te brengen gemeentelijk plan (vastgesteld door het CMT (Concern Managementteam)) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA (Eenduidige Normatiek Single Information Audit). Daarin 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 informatiebeveiligingsbeleid geldt voor alle processen van de gemeente 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 gemeente op het gebied van informatieveiligheid

- Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de bedrijfsprocessen van de gemeente en de basis voor het verwerken van vertrouwelijke gegevens ter bescherming van privacy en rechten van haar inwoners en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

De komende jaren zet de gemeente Venray in op verbeteren van informatiebeveiliging en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Informatiebeveiligingsbeleid voor de jaren 2020 tot 2023'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in een jaarlijks bij te stellen plan.

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat het CMT 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 zijn 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 [1] 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 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] Deze principes zijn gelijk met de BIO van kracht gegaan, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op 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.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk het register informatiebeveiligingsincidenten waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook 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 gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] 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 ISO en de BIO.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de 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 jaarlijks planmatig aangepakt.

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente 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.
Dit informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI . Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
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] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

2.6 Uitgangspunten

Het bestuur, het CMT en AMT (Afdelingsmanagement) spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Het CMT maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het CMT dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

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 een informatiebeveiligingsbeleid van en voor de hele gemeente. 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 van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van de teammanagers. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Venray 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 bijbehorende plan het fundament onder een betrouwbare informatievoorziening. In dit plan 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. 'Plan, do, check en act' 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 en vastgesteld.
- Iedere medewerker, 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 informatiebeveiligingsbeleid vast.
- Het CMT stelt jaarlijks een informatiebeveiligingsplan vast.
- Het CMT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het CMT is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers 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 het CMT, 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 teammanagers 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 gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Teammanagers 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.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een plan opgesteld, gebaseerd op:
    - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - het dreigingsbeeld gemeenten van de IBD;
    - De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

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 is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO) 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: CMT

Het CMT zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. Het CMT zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het CMT 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.

Het CMT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het CMT draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het CMT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Venray gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teammanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle teammanagers. 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, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan het CMT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Periodiek vindt er afstemming tussen de CISO en teammanagers plaats. Voorbereiding en coördinatie van het overleg ligt bij de CISO.

Taken van de teammanagers 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, 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.

3.3 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Venray. De bestuurders en managers van de gemeente Venray 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.
Het CMT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het CMT 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 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Deze taak is belegd bij de aangewezen ENSIA-coördinator. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de daarvoor verantwoordelijke medewerkers. De teammanagers zijn verantwoordelijk voor de te leveren informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en 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 collegeverklaring aan de raad.

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

Vastgesteld op : 19 november 2024

Burgemeester en wethouders van Venray,

De burgemeester, De secretaris,

Michiel Uitdehaag Evert Voorn

Bijlage bij informatiebeveiligingsbeleid 2024-2026: DigiD-uitwerking norm B.01

In aanvulling op het informatiebeveiligingsbeleid 2024-2026 (dat integraal van toepassing is op al onze DigiD-aansluitingen) zijn voor DigiD de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen
We conformeren ons aan de laatste door Logius gepubliceerde Norm, ICT-beveiligingsassessments DigiD versie 3.0.[1]

De afzonderlijke normen worden getoetst op opzet en bestaan. Voor drie normen geldt ook dat de werking moet worden aangetoond.

Norm	Opzet	Bestaan	Werking
B.01			
B.05			
U/TV.01			
U/WA.02			
U/WA.05			
U/NW.06			
C.08			

Term	NOREA definitie	Uitleg
Opzet	Beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.	Beschrijving van maatregelen, zoals een beleid, plan of procedure die is ontworpen om een specifiek doel te bereiken. Het is een weergave van de werkelijkheid. Bewijs hiervan kan de documentatie van een procedure zijn maar bijvoorbeeld ook een netwerkplaat.
Bestaan	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen op of rond een peildatum.	Controleert of de procedure en maatregelen daadwerkelijk bestaan en werken zoals beschreven. Bewijs kan een voorbeeld zijn van de toepassing van de procedure.
Werking	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving gedurende een bepaalde periode.	Evalueert of de procedure effectief werkt in het behalen van de beoogde doelen gedurende een bepaalde periode. Bewijs bestaat uit meerdere waarnemingen, verkregen via een steekproef, die regelmatig de effectieve toepassing van de procedure over een langere periode aantonen.

Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst. Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

[1] Logius | Normenkader 3.0 voor ICT-beveiligingsassessments DigiD

Eigenaarschap
Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende teammanager eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Burgerzaken: teammanager Burgerzaken
Mijn Inkomen: teammanager Werkplein
VRiS: teammanager I&A, GEO en Informatiebeheer
Website: teammanager Burgerzaken

Functioneel beheer
Per DigiD-aansluiting is door de genoemde leidinggevende een functioneel beheerder aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.

Burgerzaken: Christel van Heumen
Mijn Inkomen: Suzan Priems
VRiS: Soon Woo
Website: Ger Vervoort

Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, t.a.v. DNSSEC) en de beoordeelde releases (C.08).
Tweemaal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk leidinggevende.

Technisch
Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.