Bedrijfsvoeringseenheid Bommelerwaard

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 767

25 juli 2023

Officiële uitgave van de gemeenschappelijke regeling Bedrijfsvoeringseenheid Bommelerwaard

Informatiebeveiligingsbeleid Bommelerwaard 2023 – 2026

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot en met 2026 voor de Bedrijfsvoeringseenheid Bommelerwaard en de gemeenten Maasdriel en Zaltbommel (hierna: de BVEB en de beide gemeenten) en vervangt het in 2021 vastgestelde Informatiebeveiligingsbeleid 2020 - 2021. 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 2023 - 2026 zetten de BVEB en de beide gemeenten 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).

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 het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid wordt gesteld. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn. Tot slot is hoofdstuk 4 bedoeld voor Evaluatie, Controle en Verantwoording waardoor de PDCA-cirkel rond is.

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 BVEB en de beide gemeenten 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 bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

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

De visie op informatieveiligheid is dat informatieveiligheid een integraal onder deel is van de kwaliteit van de informatievoorziening en als zodanig ook een onderdeel vormt van integraal management. Als onderdeel van het integraal management wordt in de context van dit beleid expliciet risk management genoemd. Bij de implementatie van BIO is het identificeren en managen van risico namelijk een belangrijke steunpijler. In de praktijk betekent dit dat informatiebeveiliging onlosmakelijk verbonden is met informatiebeleid en –planning en onderdeel vormt van beheer en ontwikkeling van informatiesystemen. Het doel is dat informatiebeveiliging in de pas loopt met de gemeentelijke ambities en direct bijdraagt aan een plezierige en veilige leef-, woon- en werkomgeving voor de regio. Voor wat betreft de kernwaarden staan vertrouwen en veiligheid eveneens hoog in het gemeentelijke vaandel. Het zal duidelijk zijn dat informatieveiligheid steunt op en ondersteunend is aan (de verwezenlijking van) deze kernwaarden!

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het Strategisch Informatiebeveiligingsbeleid voor de jaren 2023 tot en met 2026. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan. Evaluatie van het beleid vindt plaats aan het einde van de looptijd. Hierbij dient opgemerkt te worden dat eerder vastgesteld informatiebeveiligingsbeleid onverminderd van kracht blijft tot dat opvolgend beleid is vastgesteld.

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 normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de afdelingsmanagers 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. Door de komst van de nieuwe ISO27002 is de binnen de overheid afgesproken BIO-evaluatie in 2023 vervroegd naar 2022. Zo zal in 2023 een vernieuwde BIO 2.0 verschijnen, met daarin de evaluatie en structuuraanpassing als gevolg van de nieuwe ISO27002. Deze aanpassingen zullen we dan volgen.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging die hieronder zijn opgenomen vormen 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.

2.2.3 Risk management en Risico bereidheid

Binnen het risk management zal een kader geformuleerd worden waarbinnen het management haar risico-beoordeling kan uitvoeren. Dit kader waarborgt dat bij het realiseren van beleidsdoelen op een gepaste wijze met het risico omgegaan wordt. Daartoe zal de directie een risico-bereidheid formuleren met betrekking tot Privacy en Security risico's welke de gemeentes en BVEB bereid zijn te lopen en wanneer het nemen van maatregelen noodzakelijk zal zijn.

2.2.4 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 dit beleid in de vorm van een Jaarplan informatiebeveiliging.

2.2.5 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem 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

1) *Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)*

2) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

niveaus van beveiligen. Door de komst van de nieuwe ISO27002 zal in 2023 een vernieuwde BIO 2.0 verschijnen, met daarin de evaluatie en structuuraanpassing als gevolg van de nieuwe ISO27002. 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 dit beleid zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen. Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) en/of Proces Automatisering (PA) ingezet voor besturing van industriële toepassingen; hierbij kun je denken aan besturing van bruggen, sluizen, camera's, pompen, gemalen en verkeerslichten, maar ook gebouwbeheersystemen. Dit is in tegenstelling tot ICT de industriële automatisering genoemd. Het beveiligingsbeleid van de gemeente is ook van toepassing op de bescherming van PA en de afdelingen/teams die zich met PA bezighouden.

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. Dit leidt tot een compact beleidsplan welke periodiek wordt vertaald in jaarplannen informatiebeveiliging. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven Informatiebeveiligingsplan.

2.5 Scope informatiebeveiliging
De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, 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 strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor DigiD, BRP, PNIK, SUWI en de Wpg. 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. Uit praktische overwegingen wordt bewust in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten
Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management 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 management 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 beleid voor Informatievoorziening en Automatisering 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 Bedrijfsvoeringseenheid en de beide gemeenten, bepaalde informatie is van vitaal en kritiek belang. Het college is eindverantwoordelijke voor de informatiebeveiliging;
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Bedrijfsvoeringseenheid en de beide gemeenten 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 (proces)eigenaar van de informatie;
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening 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 Bedrijfsvoeringseenheid en de beide gemeenten stellen de benodigde mensen en middelen beschikbaar om hun eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid;
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden 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 stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast;
- De directie stelt jaarlijks het informatiebeveiligingsplan vast;
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van specifieke tactische maatregelen en aanvullend beleid, die aanvullend zijn op dit strategisch beleid. De vaststelling hiervan vindt plaats door de in de BIO genoemde verantwoordelijken;
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringssystemen die onder hun verantwoordelijkheid valt;
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken;
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen;
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn;
- De afdelingsmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basisregistraties (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;
- Voor het gebruik en beheer van Suwinet binnen Maasdriel wordt jaarlijks een apart beveiligingsplan opgesteld dat wordt vastgesteld door de directie.
- Alle medewerkers van de BVEB en de beide gemeenten worden getraind in het gebruik van beveiligingsprocedures;
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie;
- Afdelingsmanagers 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. Afdelingsmanagers voeren quickscans uit om het Basis Beveiligingsniveau (BBN) te bepalen van de informatiebeveiliging op basis van de BIO om zo risico-afwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

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

3. Organisatie & Governance

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, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. De adviezen hebben hier het karakter van een interne review waarbij het management steeds verantwoordelijk blijft voor de opvolging hiervan. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing door directie

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen primair onder de bevoegdheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. 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 periodiek het gewenste niveau van continuïteit en vertrouwelijkheid vast op basis van de risico-classificaties. De directie draagt zorg voor het (doen) uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt binnen de BVEB en de beide gemeenten gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering door management

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden en teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij te beschikken over passende bevoegdheden en ondersteuning vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Alle processen, systemen, data, applicaties moeten minimaal 1 eigenaar hebben; er is dus altijd iemand verantwoordelijk. Afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door het onderwerp informatiebeveiliging periodiek te bespreken in het afdelings-/teamoverleg.

Taken van de afdelingsmanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures;
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Het binnen de eigen afdeling/team 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;

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

3.3.1 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Aanvullend op dit beleid zijn extra normen van toepassing zoals opgenomen in de bijlage van dit document. Jaarlijks wordt een ENSIA-coördinator aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingsmanagers. De afdelingsmanagers 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 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 BVEB en de beide gemeenten en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de BVEB en de beide gemeenten informatiebeveiliging serieus nemen en het onderdeel laten zijn van de ambities om informatie van inwoners adequaat te beschermen.

Inwerkingtreding
Dit informatiebeveiligingsbeleid treedt een dag na bekendmaking in werking. Het Informatiebeveiligingsbeleid Bedrijfsvoeringseenheid Bommelerwaard en de gemeenten Maasdriel en Zaltbommel 2020 – 2021 wordt per die datum ingetrokken. Het beleid wordt tweejaarlijks geëvalueerd en indien nodig herzien. Aanpassingen aan dit beleid worden bekendgemaakt. De meest actuele versie van het beleid is te vinden op de website van de gemeente.

Aldus vastgesteld in de bestuursvergadering van 4 juli 2023,

B. (Benno) Cerutti
Directeur

C.A.H. (Kees) Zondag
Voorzitter

Bijlage 1: DigiD-uitwerking norm B.01

In aanvulling op dit informatiebeveiligingsbeleid (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.
- 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.

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/Afdelingshoofd**
  - ➢ **iBurgerzaken Maasdriel: Teammanager Publieke Dienstverlening**
  - ➢ **iBurgerzaken Zaltbommel: Afdelingshoofd Publiekszaken**
  - ➢ **Zaaksysteem Maasdriel/Zaltbommel: Teammanager I&A BVEB**

  eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer:
- Per DigiD-aansluiting is door de genoemde T**eammanager/Afdelingshoofd** een **Functioneel Beheerder**
  - ➢ **Functioneel Beheerder iBurgerzaken Maasdriel**
  - ➢ **Functioneel Beheerder iBurgerzaken Zaltbommel**
  - ➢ **Functioneel Beheerder Zaaksysteem BVEB**

  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.
- 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, tav 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 **Teammanager/Afdelingshoofd**.

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.