Informatiebeveiligingsbeleid Gemeente Weert 2023-2024

Verantwoordelijke: [redacted]

Auteur: [redacted]

1. Inleiding

Deze beleidsnota beschrijft het strategische informatiebeveiligingsbeleid voor de jaren 2023 - 2024 en vervangt het op 10 december 2019 vastgestelde "GBD-200 - Informatiebeveiligingsbeleid Gemeente Weert versie 3.0".

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Deze aanvullingen zijn als Standaard Operatie Procedures (SOP's) en werkinstructies (WI's) te vinden op OCTO en worden beheerd in de LIAS-Content Portal (ISMS-tool en kwaliteitssysteem in gebruik bij Gemeente Weert).

Met dit strategische informatiebeveiligingsbeleid 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 strategische 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, zie bijlage A.

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 afdelingshoofden, 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 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 binnen informatie(systemen) te waarborgen. 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 maar heeft ook betrekking op het politiek bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het informatiebeveiligingsbeleid 2023-2024. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP). Dit plan ligt vast, en wordt beheerd, in het door de Gemeente Weert gebruikte Information Security Management System (ISMS).

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. Dit betekent dat de Gemeente haar informatiebeveiligingsbeleid en haar verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (middels ENSIA) baseert op deze BIG. De werkzaamheden die voor de BIG zijn verricht zijn al grotendeels in lijn met de BIO. Dat wil zeggen dat de afdelingshoofden 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 zij op voorhand keuzes en continu afwegingen maken 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 (zie bijlage A)

De 10 principes van informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader[1] BIO en gaan over de waarden die de Gemeente Weert zich 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 Dreigingsbeeld Nederlandse Gemeenten

Het dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (Bijlage B) 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 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 nadrukkelijke input bij het actualiseren van het beleid.

2.2.5 Classificatie van gegevens

Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie bekend is. Classificatie van informatie in termen van vereiste vertrouwelijkheid, integriteit en beschikbaarheid.

Het begrip informatiebeveiliging heeft aldus betrekking op:

- Beschikbaarheid: het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen, zoals

- het management en medewerkers informeren over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- de waarde tonen van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- mede gerelateerd aan alle relevante en specifiek geldende wet- en regelgeving en contractuele verplichtingen.

De eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde van elk van de geïdentificeerde middelen.

2.2.6Toegangsvoorziening

De gemeente heeft maatregelen getroffen om ongeoorloofde toegang (zowel fysiek als logisch) tot haar pand en informatie verwerkende faciliteiten te voorkomen. De expliciete maatregelen die getroffen zijn hiervoor, zijn opgenomen en beschreven in relevantie documentatie. Toegang geschiedt bij de gemeente te allen tijde op basis van ‘need-to-access’. Dit betreft interne systemen en faciliteiten, maar wordt ook toegepast binnen producten die de gemeente ontwikkelt.

Dat vereist naast toegangsbeleid ook beheer van toegangsrechten om toegang voor bevoegde gebruikers te bewerkstelligen en onbevoegde toegang tot systemen en diensten te voorkomen en waar nodig gebruik te maken van een beveiligde inlogprocedure. Gebruikers zijn verantwoordelijk voor het beschermen van hun authenticatie-informatie zoals wachtwoorden.

2.2.7 Kwetsbaarhedenbeheer

De gemeente werkt vanuit een veilige IT-omgeving en ontwikkelt producten die voldoen aan de hoogste eisen van informatiebeveiliging. Wanneer er kwetsbaarheden worden gedetecteerd, neemt de gemeente hier via diverse fora, specialisten en koppelingen (RSS-feeds) notie van. Het dichten van deze kwetsbaarheden zal op basis van een risicoanalyse in de tijd weggezet worden.

De gemeente laat zowel op de fysieke locatie als op haar producten met regelmaat pentests uitvoeren.

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.

De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan (LIAS-Content) zal deze structuur volgen.

2.4 Plaats van het strategische beleid

Het strategische 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 uitgewerkt in het gemeentelijk Informatiebeveiligingsplan (LIAS-Content) en gedeeltelijk gepubliceerd (intern) in de werkgroep Informatiebeveiliging & privacy op OCTO.

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 (zowel vast als tijdelijk, intern of extern) en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch gemeentelijke 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.

2.6 Uitgangspunten

Het bestuur, de directie en het afdelingsmanagement speelt 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 hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management een 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 juist identificeren en classificeren van data in informatiesystemen;
- Het waarborgen van veilige en geüpdatete informatiesystemen;
- Het adequaat reageren op (beveiligings)incidenten;
- Het beschermen van kritieke bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van alle medewerkers, burgers, gasten, bezoekers en externe relaties;
- 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&W 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. De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Weert hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze 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&W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.

- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoording 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 of afdelingsplannen.
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingshoofden zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, BRO, SUWI, BAG, BGT en WOZ) en toekomstige basisregistraties belangrijk zijn in 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 we gesteld hebben.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Alle medewerkers van de gemeente Weert hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid. Identificatie van incidenten of het niet voldoen aan het gestelde in dit beleid dient gemeld te worden aan de CISO. Alle medewerkers worden actief geïnformeerd over dit beleid en worden verwacht kennis te nemen van de inhoud.
- Afdelingshoofden 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. Afdelingshoofden voeren elk half jaar quickscans informatiebeveiliging uit op basis van de BIO om deze 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.
- 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 afdelingshoofden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse

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 ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: Directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingshoofden 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.

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

3.2 Uitvoering: Afdelingshoofden

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden, 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. Afdelingshoofden rapporteren over de door hun tactisch- en operationeel uitgevoerde informatiebeveiliging activiteiten aan de directie. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 1 keer per jaar het onderwerp informatiebeveiliging te bespreken in het CMT.

Taken van de afdelingshoofden 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 informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de Gemeente Weert. De bestuurders en directeuren van de Gemeente Weert 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.

3.4 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA systematiek. Dat betekent dat een ENSIA coördinator wordt aangewezen, deze

zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden 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 Collegeverklaring aan de Raad.

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

Samenvatting

Met het beleidsdocument informatiebeveiliging 2023 – 2024 geeft het college van B&W de kaders en uitgangspunten aan voor het vormgeven en onderhouden van informatiebeveiliging. De uitwerking van dit beleid naar de organisatie ligt bij de directie en de proceseigenaren. De proceseigenaren sturen op risico’s, bepalen welke beveiligingsmaatregelen nodig zijn, draagt dit uit naar hun organisatieonderdelen.

3.5 Bijlagen

Bijlage A: De 10 bestuurlijke principes voor informatiebeveiliging

Bijlage B: Dreigingsbeeld informatiebeveiliging

Vastgesteld op : [datum] door het college van Gemeente Weert.

[Ondertekening]

---

(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.*