GEMEENTE WEST BETUWE

GEMEENTEBLAD

Officiële uitgave van de gemeente West Betuwe

Nr. 514921

27 november 2025

Strategisch informatiebeveiligingsbeleid 2025-2029

1. Het strategische informatiebeveiligingsbeleid 2025-2029 vast te stellen;
2. Mandaat te verlenen aan de gemeentesecretaris om onderliggende (tactische) beleidsdocumenten en procedures uit te (laten) werken en vast te stellen;
3. Het strategisch informatiebeveiligingsbeleid 2021-2024 in te trekken.

1. Visie en Ambitie op informatieveiligheid

De gemeenten Culemborg, Tiel, West Betuwe en de Bedrijfsvoeringsorganisatie West-Betuwe (BWB) staan gezamenlijk voor grote maatschappelijke opgaven en ontwikkelingen die nieuwe antwoorden en vaardigheden vereisen. Technologische innovaties, digitalisering en de toepassing van kunstmatige intelligentie kunnen een belangrijke bijdrage leveren aan het realiseren van deze opgaven. Daar willen en zullen wij meer gebruik van maken.

Deze opgaven en ontwikkelingen kunnen echter alleen succesvol worden gerealiseerd in een veilige en betrouwbare omgeving. Een omgeving die ruimte biedt aan technologische vooruitgang en innovatieve toepassingen faciliteert. Dit maken wij mogelijk door informatiebeveiliging slim en doelgericht in te zetten.

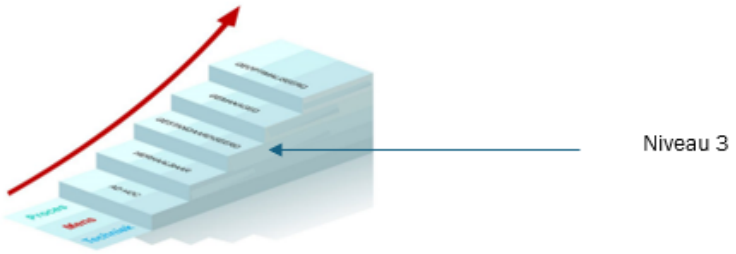
De gemeenten ambiëren een toekomstgerichte informatievoorziening die bijdraagt aan een betrouwbare organisatie. Het borgen van informatieveiligheid is hiervoor een essentiële randvoorwaarde.

Om deze basis op orde te brengen en te houden, sluiten wij aan bij de landelijke Baseline Informatiebeveiliging Overheid (BIO), die duidelijke kaders en richting biedt. Door de BIO te volgen voldoen wij aan wet- en regelgeving, en beschikken we over voldoende kennis en capaciteit om proactief in te spelen op nieuwe ontwikkelingen. Zo verkleinen wij risico's tot een acceptabel niveau, in lijn met de bestuurlijke en organisatorische ambities. Voor inwoners, bedrijven en (keten)partners willen wij daarmee een betrouwbare overheid zijn. De informatiebeveiligingsorganisatie ondersteunt dit door inzicht te bieden in zowel kansen als dreigingen.

Ons ambitieniveau voor informatiebeveiliging is vastgesteld op volwassenheidsniveau 3 (Gedefinieerd), voor zover dit binnen onze eigen invloedsfeer ligt. Dit niveau willen wij uiterlijk eind 2028 hebben bereikt. Niveau 3 geldt tevens als het minimum om te kunnen stellen dat wij voldoen aan de BIO, de verplichtingen uit de NIS2-richtlijn en de aankomende Cyberbeveiligingswet, die gemeenten verplichten om informatiebeveiliging aantoonbaar op orde te hebben en ketenverantwoordelijkheid te borgen.

Met deze 'basis op orde' is informatiebeveiliging organisatiebreed geborgd en wordt een belangrijke randvoorwaarde vervuld voor zowel onze dienstverlening als onze strategische doelen. Waar wet- en regelgeving hogere eisen stelt aan beheersing, meting (niveau 4) of continue verbetering (niveau 5), zal een hoger volwassenheidsniveau worden toegepast. Een voorbeeld hiervan is de Wet politiegegevens, waarin voor het verwerken van deze gegevens striktere voorwaarden gelden.

Samenvattend: Niveau 3 betekent dat beheersingsmaatregelen zijn gedocumenteerd, gestructureerd en geformaliseerd worden uitgevoerd, en dat de uitvoering aantoonbaar en toetsbaar is. De concrete uitwerking om dit niveau te bereiken is opgenomen in het Informatiebeveiligingsplan.



Figuur 1: Figuur1: volwassenheidsmodel informatiebeveiliging Norea schaal 1 tot en met 5.
Volwassenheidsmodel informatiebeveiliging (nba.nl)

2. Inleiding

Digitalisering verandert onze samenleving voortdurend en biedt kansen. De grote impact van digitalisering volgt uit de grote verwevenheid ervan in alle beleidsonderdelen van de overheid, van het fysiek domein tot democratie. Daarin helpt digitalisering om de samenleving beter te maken en de grote opgaven die er liggen aan te pakken. Dat gaat niet vanzelf er is nog veel te doen om de kansen van gisteren goed te pakken en klaar te zijn voor die van morgen.

Het is ook duidelijk dat er risico's en schade met digitalisering meekomen. Kwetsbaarheden en dreigingen nemen in het digitale domein toe. Landelijk presenteren het Nationaal Cyber Security Center (NCSC), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Informatie Beveiligingsdienst Gemeenten (IBD) dreigingsbeelden rondom integrale veiligheid, informatieveiligheid en cybersecurity. Deze geven een duidelijk beeld van ontwikkelingen, dreigingen en risico's die ook voor onze organisatie relevant zijn. Dit vraagt om extra inspanningen om de weerbaarheid op het gebied van informatieveiligheid te versterken en te borgen.

Dit strategisch informatiebeveiligingsbeleid 2025-2029 is het beleidskader om informatie te beschermen, zodat de organisatie voldoet aan relevante wet- en regelgeving. Het draagt bij aan de weerbaarheid en wendbaarheid en aan een toekomstbestendige bedrijfsvoering en dienstverlening. Het strategisch beleid is de basis voor het tactische beleid en geeft daarmee de organisatie richting voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Dit beleid is geldig vanaf 2025 tot en met 2029 en vervangt de vorige versies van het strategische informatiebeveiligingsbeleid. Aanpassing van het beleid kan plaatsvinden op basis van voortschrijdend inzicht, zoals wijziging van organisatiedoelen, feedback en ervaring ten aanzien van de werkbaarheid, doelmatigheid en effectiviteit op basis van de uitvoering van het beleid, de stand van de techniek (nieuwe beveiligingstechnieken), nieuwe dreigingen of aanvalstechnieken en veranderingen aan wet- en regelgeving. Het informatiebeveiligingsbeleid van onze organisatie voldoet aan de geldende wet- en regelgeving en wordt toegepast volgens het principe "pas toe of leg uit".

2.1 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernbegrippen daarbij zijn de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van (persoons)gegevens en andere informatie.

De primaire doelstelling van informatiebeveiliging is het aantoonbaar beheersen van risico's door middel van een risicogebaseerde aanpak. Hiervoor wordt momenteel een managementsysteem voor informatiebeveiliging (ISMS) ingericht, geïmplementeerd, onderhouden en continu verbeterd. Deze aanpak draagt bij aan een moderne en veilige informatievoorziening en een effectief besturingsmodel.

Informatiebeveiliging omvat organisatorische, fysieke, digitale én menselijke aspecten. De mens vormt daarbij de belangrijkste schakel. Om weerbaarheid te versterken en te behouden, is voortdurende aandacht voor al deze aspecten noodzakelijk. Informatieveiligheid is en blijft een bestuurlijke verantwoordelijkheid.

Informatiebeveiliging is geen doel op zich, maar staat altijd in verhouding tot de gemeentelijke doelstellingen en de werkzaamheden die nodig zijn om deze te realiseren.

2.2 Doel en reikwijdte van dit beleid

Het strategisch informatiebeveiligingsbeleid 2025–2029 vormt het beleidskader voor de bescherming van informatie, zodat de organisaties voldoen aan hun zorgplicht en aan de relevante wet- en regelgeving. Dit beleid is gericht op de verdere implementatie van de BIO, draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan het behalen van de organisatiedoelstellingen. Het strategisch beleid is de basis voor het tactische beleid en geeft daarmee richting voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Dit beleid is van toepassing op alle processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeenten Culemborg, Tiel, West Betuwe en BWB en daarnaast voor dit onderdeel betrokken externe partijen zoals leveranciers, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het (gemeente)bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatiebeveiliging gedurende de hele levenscyclus van informatiesystemen.

Binnen de gemeente wordt naast kantoorautomatisering ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering. Op alle Proces Automatiseringssystemen (PA) die binnen de gebouwen en in de publieke ruimte van de gemeente worden gebruikt en waarvan de gemeente de eigenaar is, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of verkeer regel installaties, pompen en gemalen is dit beveiligingsbeleid ook van toepassing.

2.3 Eigenaarschap en evaluatie

Het college van burgemeester en wethouders van de deelnemende gemeenten is verantwoordelijk voor:

- **Beleidsbepaling**: het vaststellen van dit beleid, het actief uitdragen van de uitgangspunten en het toezien op de naleving door het lijnmanagement.
- **Randvoorwaarden**: het beschikbaar stellen van voldoende middelen en capaciteit, en het ondersteunen van de implementatie en naleving van dit beleid binnen de organisatie.

De Chief Information Security Officer (CISO) is door het college gemandateerd om dit document te beheren en fungeert als inhoudelijk verantwoordelijke voor de actualiteit en toepasbaarheid van het Informatiebeveiligingsbeleid. De CISO evalueert dit beleid jaarlijkse en past het waar nodig aan op basis van veranderde inzichten, nieuwe wet- en regelgeving of technologische ontwikkelingen. De mandatering waarborgt dat de CISO zelfstandig kan optreden binnen de kaders van het college en tegelijkertijd verantwoordelijk blijft voor de coördinatie, implementatie en bewaking van het beleid.

Bij significante wijzigingen wordt het beleid opnieuw ter vaststelling aan het college voorgelegd, zodat bestuurlijke verankering is geborgd. Op die manier blijft het beleid actueel, passend bij de ambities van de organisatie en in lijn met landelijke kaders zoals de BIO en de NIS2-richtlijn.

2.4 Communicatie

Na vaststelling via het GDO door de directie van BWB en de colleges van burgemeester en wethouders van de gemeenten Culemborg, Tiel en West Betuwe wordt dit beleid gepubliceerd en via het lijnmanagement onder de aandacht gebracht van alle medewerkers. Waar relevant wordt het tevens gedeeld met externe partijen, zodat ook zij op de hoogte zijn van de geldende kaders en verplichtingen.

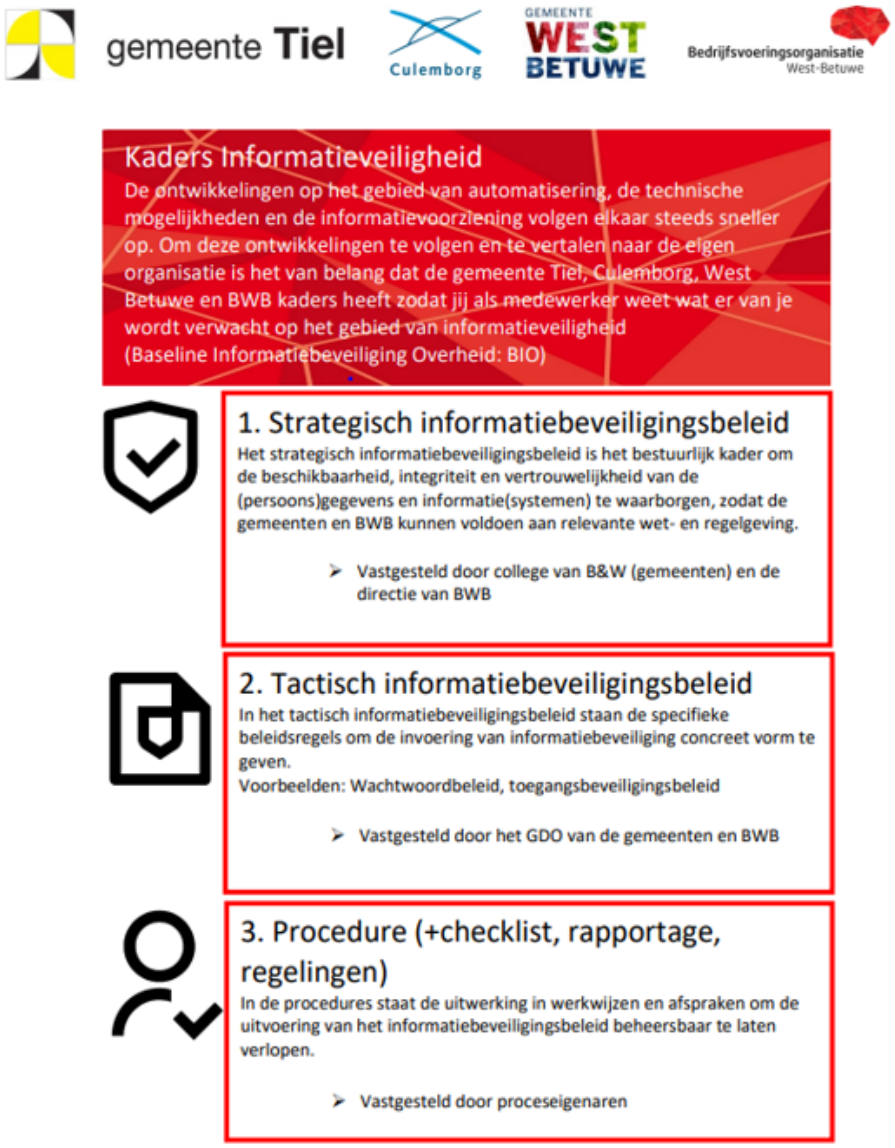
3. Beleidskader informatiebeveiliging

3.1 Plaats van dit beleid

Het strategisch informatiebeveiligingsbeleid is in lijn met de relevante nationale en Europese wet- en regelgeving (zoals de BIO en voor zover van toepassing de NIS2-richtlijn). Het beleid kent een gelaagde opzet met een duidelijke doorvertaling van strategie naar uitvoering:

1. Strategisch informatiebeveiligingsbeleid: legt de strategische uitgangspunten, doelen en kaders vast (dit document).
2. Tactische beleidsdocumenten: werken de strategische uitgangspunten uit in organisatiebrede kaders en onderwerpspecifieke beleidsregels die de implementatie van informatiebeveiliging verplicht stellen. Voorbeelden zijn het tactisch kader voor toegang tot digitale informatie, de kaders voor screening van personeel, wachtwoordbeleid en het informatiebeveiligingsplan.
3. Operationele documenten: vertaling van het tactische beleidsdocumenten naar de praktijk zoals procesbeschrijvingen, operationele procedures en werkinstructies.

De strategische uitgangspunten vormen de basis voor alle vervolgdocumenten. Deze uitgangspunten worden in de tactische laag geconcretiseerd naar toepasbare regels en richtlijnen en komen in de operationele laag terug als uitvoerbare processen en procedures. Hiermee is geborgd dat de strategische keuzes consistent worden doorgevoerd in beveiligingsplannen, processen en werkinstructies, en dat dezelfde uitgangspunten tevens herkenbaar zijn in andere relevante beleidsdocumenten binnen de organisatie.



Figuur 2: Flyer informatieveiligheid beleidsvelden

3.2 Wettelijke basis

3.2.1 Cyberbeveiligingswet

Om de fysieke, digitale en economische weerbaarheid te versterken, heeft de Europese Unie de Network and Information Security Directive (NIS2) vastgesteld. In Nederland wordt deze richtlijn geïmplementeerd via de Cyberbeveiligingswet (Cbw). Gemeenten zijn, net als andere overheidsinstanties, binnen deze wet aangewezen als essentiële entiteiten.

De belangrijkste reden voor deze aanwijzing is dat gemeenten verantwoordelijk zijn voor onderdelen van industriële automatisering, zoals verkeersregelinstallaties, smartcity-toepassingen, afvalverwerking, pompen, gemalen en parkeergarages. Digitale veiligheid is daarmee een wettelijke verplichting geworden, die verder reikt dan alleen de beveiliging van kantoorautomatisering.

Het toezicht is daarnaast versterkt en verbreed: naast controles achteraf voert de toezichthouder ook inspecties en audits vooraf uit op de digitale beveiliging van gemeenten. De Rijksinspectie Digitale Infrastructuur (RDI) is hierbij aangesteld als bevoegde toezichthouder.

Gemeenten hebben onder de Cyberbeveiligingswet de volgende verplichtingen:

- **Registratieplicht**: inschrijving als essentiële entiteit in het landelijke register.

- **Zorgplicht**: nemen van passende technische en organisatorische maatregelen om de digitale weerbaarheid te waarborgen.
- **Meldplicht**: het tijdig (binnen 24 uur) melden van significante (cyber)incidenten bij de toezichthouder.
- **Toezicht**: gemeenten staan onder toezicht van de RDI, die zowel preventief (audits) als repressief (handhaving) kan optreden.

3.2.2 Baseline Informatiebeveiliging Overheid 2

De Baseline Informatiebeveiliging Overheid 2 (BIO2) vormt het nieuwe kader voor informatiebeveiliging en volgt de BIO 1.04 op. De BIO2 is geen wetgeving op zichzelf, maar in de Cyberbeveiligingswet staat dat aanvullende regels voor beveiliging via een Algemene Maatregel van Bestuur kunnen worden gesteld, wat dan de BIO2 is. De BIO2 heeft als doel NIS2/Cyberbeveiligingswet-compliant te zijn. Dat betekent dat het volgen van de BIO2 onze organisatie helpt om aan de Cyberbeveiligingswet te voldoen.

Dit strategische informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid BIO 2 De BIO 2 is gebaseerd op:

- NEN-ISO/IEC 27001:2023
- NEN-ISO/IEC 27002:2022
- En lijst met aanvullende overheidsmaatregelen

3.2.3 De Cybersecurity Implementatie Richtlijn (CSIR)

Onze organisaties gebruiken de BIO als beveiligingsnorm voor de beveiliging van onze kantoorautomatisering. Voor het beveiligingen van industriële automatisering en/of procesautomatiseringssystemen bestaan aanvullende beveiligingseisen die niet in de BIO staan. Voor de bescherming van Proces Automatisering is met name de Cybersecurity Implementatie Richtlijn (CSIR) van toepassing. Deze CSIR-richtlijn is namelijk speciaal ontwikkeld om objecten (waterzuiveringsinstallaties, gemalen, bruggen, keringen, sluizen, etc.) te beveiligen.

3.3 Handvatten voor de rol van de bestuurder

De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO en gaan over de principes op basis waarvan de bestuurder denkt, bestuurt en handelt. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers.

De 10 principes zijn:

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.

Deze 10 principes van VNG/IBD [1] staan nader uitgewerkt in de uitgewerkte rolverdeling van hoofdstuk 5 en in het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

3.4 Uitgangspunten

Dit hoofdstuk beschrijft de uitgangspunten en deze zijn de belangrijkste normen en waarden die de gemeenten en BWB nastreven bij het beveiligen van haar informatie en de hiervoor minimale benodigdheden.

1) De Informatiebeveiligingsdienst voor gemeenten (IBD) onderdeel van Vereniging van Nederlandse Gemeenten (VNG). **https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/**

3.4.1 Leiderschap en continu proces

- Het bestuur, de directie en de leidinggevenden dragen dit beleid uit en sturen op de implementatie van dit beleid.
- Regels, verantwoordelijkheden en bevoegdheden die relevant zijn voor informatiebeveiliging zijn toegekend en gecommuniceerd binnen de organisatie.
- Benodigde middelen en competenties worden vastgesteld en beschikbaar gesteld om eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan dit beleid.
- Om het informatiebeveiligingsproces te structureren wordt gebruikgemaakt van een managementsysteem (ISMS), gebaseerd op het Plan-Do-Check-Act (PDCA)-model. Binnen dit systeem worden op verschillende niveaus rapportages opgesteld en gedeeld, variërend van de proceseigenaar tot en met de directie en het bestuur. Op deze manier is de voortgang van het informatiebeveiligingsproces geborgd en krijgt ieder niveau de informatie die nodig is om zijn verantwoordelijkheid te kunnen nemen.
- Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én coördinatie wordt de kwaliteit van de informatiebeveiliging verankerd en verbeterd binnen de organisatie.
- Het managementsysteem voor informatiebeveiliging moet o.a. bevatten de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van het managementsysteem van informatiebeveiliging.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging.
- Tijdens Planning & Control-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 auditplannen.
- Elk bedrijfsproces en informatiesysteem dat wordt gebruikt, heeft of krijgt binnen het ISMS een eigenaar (lijnmanager). Deze eigenaar bepaalt de waarde van de informatie die het proces of systeem bevat. De primaire verantwoordelijkheid voor de bescherming van deze informatie ligt bij de eigenaar, die verantwoording aflegt over de beveiliging ervan.
- De rol van de coördinator van informatiebeveiliging (Chief Information Security Officer: CISO) is ingevuld. De CISO ondersteunt vanuit een onafhankelijke positie het bestuur en management bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
- Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT, BRO) 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.

3.4.2 Risicobeheersing

- Informatiebeveiliging is onlosmakelijk verbonden met risicomanagement. Risico's worden in kaart gebracht en door de proceseigenaar en de CISO afgewogen. Indien een risico de reikwijdte van een proces of organisatieonderdeel overstijgt, vindt de afweging en eventuele acceptatie plaats op management- of directieniveau.
- De inrichting van informatiebeveiliging is procesgestuurd en risicogebaseerd. Beveiligingsmaatregelen worden vastgesteld volgens een voorgeschreven risicomanagementmethodiek, waarbij geldende wet- en regelgeving (waaronder BIO, NIS2 en AVG) altijd leidend is.
- Om te waarborgen dat informatie over risico's en incidenten actueel, volledig en juist is, worden deze centraal vastgelegd en periodiek geactualiseerd in het Information Security Management System (ISMS). Dit systeem ondersteunt tevens de aantoonbaarheid richting auditors en toezichthouders.
- Informatiebeveiligingsincidenten worden afgehandeld volgens een gestandaardiseerd proces. Ernstige incidenten en datalekken worden conform de wettelijke verplichtingen tijdig gemeld aan de bevoegde toezichthouders en, indien van toepassing, aan betrokkenen.

3.4.3 Cyberweerbaarheid

- De gemeenten Culemborg, Tiel, West Betuwe en BWB nemen technische en organisatorische maatregelen om de organisaties te beschermen tegen incidenten en cyberdreigingen, om deze tijdig te detecteren, te herstellen en de impact te beperken. Hierbij wordt ingezet op logging, geautomatiseerde detectie, analyse en waar mogelijk automatische respons.
- De organisaties versterken hun cyberweerbaarheid door kritieke processen te identificeren, risico's te beoordelen en passende beveiligingsmaatregelen te treffen (bedrijfscontinuïteit).

- Voor de borging van de bedrijfscontinuïteit volgen wij de geldende wet- en regelgeving en de richtlijnen en adviezen van de Vereniging van Nederlandse Gemeenten (VNG).
- Werkinstructies, procedures en beleid worden periodiek getest om effectiviteit en actualiteit te waarborgen.

3.4.4 Digitaal vaardig gedrag

- Het lijnmanagement heeft voortdurend aandacht voor het vergroten van de digitale vaardigheden en het veilige gedrag van medewerkers, om zo de menselijke schakel te versterken.
- Medewerkers dienen verantwoord om te gaan met (persoons)gegevens en andere informatie. Een bewustwordingsprogramma ondersteunt hen hierbij.
- Waar relevant voor de uitvoering van werkzaamheden worden medewerkers getraind in het toepassen van beveiligingsprocedures.
- Iedere medewerker – vast of tijdelijk, intern of extern – die toegang heeft tot informatie en systemen, is verplicht deze te beschermen tegen ongeautoriseerde toegang, gebruik, wijziging, openbaarmaking, vernietiging, verlies of overdracht. Bij (vermeende) inbreuken geldt een meldplicht. Deze verplichting geldt eveneens voor raads- en commissieleden die toegang hebben tot gemeentelijke informatie of systemen.

3.4.5 Overige uitgangspunten

- De verantwoordelijkheid voor informatiebeveiliging eindigt niet bij de voordeur van onze organisatie. Ook zaken als verbindingen met externe partijen en leveranciers zijn van belang. Er worden gelijkwaardige eisen gesteld aan leveranciers en externe partijen, zoals dit ook voor de interne situatie zou gebeuren. Uitgangspunt hierbij is dat we niet alleen inzetten op de bescherming van gebouwen en (IT) voorzieningen maar sturen op het beschermen van informatie (data) ongeacht waar deze zich bevindt.
- Dit beleid dient als uitgangspunt voor:
  - het passend beheersen van informatiebeveiligings- en privacy risico's;
  - het herkennen en voorkomen van incidenten;
  - het kunnen omgaan met incidenten en calamiteiten;
  - het verhogen van de digitale weerbaarheid;
  - het voldoen aan normen en wet- en regelgeving; en,
  - het beschermen van inwoners, medewerkers en andere belanghebbenden.

3.5 Randvoorwaarden

Voor een effectieve uitvoering van dit beleid gelden de volgende randvoorwaarden:

- Er worden voldoende financiële middelen en uitvoeringscapaciteit beschikbaar gesteld om het informatiebeveiligingsbeleid en -plan uit te voeren.
- Informatiebeveiligingseisen maken structureel deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd en gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging worden actief bevorderd en geborgd op alle niveaus binnen de organisatie.
- Het informatiebeveiligingsplan wordt, indien nodig, jaarlijks geactualiseerd onder aansturing van de CISO, op basis van:
  - dit informatiebeveiligingsbeleid,
  - de resultaten van de jaarlijkse ENSIA-verantwoording,
  - overige audits (zoals de Financiële Jaarrekeningcontrole en Wpg-audit),
  - het dreigingsbeeld gemeenten van de VNG/IBD en het NCSC,
  - en de uitkomsten van uitgevoerde risicoanalyses.

4. Ontwikkelingen

4.1 Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten biedt een actueel overzicht van relevante incidenten en factoren uit het verleden, aangevuld met verwachtingen voor het heden en de nabije toekomst. Dit dreigingsbeeld vormt een belangrijk uitgangspunt voor de risicoworkshops met directie en lijnmanagement. Tijdens deze sessies wordt het gebruikt om focus aan te brengen bij het actualiseren van beleid en plannen voor informatiebeveiliging en bedrijfscontinuïteit (BCM).

4.2 Informatie uit incidenten, inbreuken op de beveiliging

Naast het landelijke dreigingsbeeld beschikken onze organisaties over een eigen systeem waarin beveiligingsincidenten en datalekken worden vastgelegd. Deze registraties maken het mogelijk om lering te

trekken uit voorvallen en worden structureel gebruikt als input bij het actualiseren en bijstellen van het informatiebeveiligingsbeleid en het Information Security Management System (ISMS).

4.3 Samenwerking met leveranciers en partners
Een belangrijk onderdeel van informatiebeveiliging is de samenwerking met externe leveranciers en partners. Onze organisaties zijn in hoge mate afhankelijk van hun dienstverlening en systemen. Daarom worden duidelijke afspraken gemaakt over beveiligingseisen, verantwoordelijkheden en incidentmeldingen. Deze afspraken worden vastgelegd in contracten en verwerkersovereenkomsten en periodiek geëvalueerd. Daarnaast wordt actief samengewerkt met ketenpartners om kennis te delen, risico's te beheersen en gezamenlijk de digitale weerbaarheid te versterken.

4.4 Bewustwording en opleiding
Menselijk handelen blijft een cruciale factor bij informatiebeveiliging. Daarom wordt blijvend geïnvesteerd in bewustwording en opleiding van medewerkers op alle niveaus. Dit gebeurt onder meer via trainingen, e-learning en voorlichtingscampagnes. Het doel hiervan is het vergroten van kennis, het stimuleren van veilig gedrag en het verkleinen van de kans op incidenten door onbedoelde fouten of onzorgvuldig handelen.

5. Organisatie van informatiebeveiliging

De gemeenten Culemborg, Tiel, West Betuwe en BWB zijn verantwoordelijk voor de beveiliging van haar informatievoorziening. Om deze verantwoordelijkheid goed in te vullen is inzicht in risico's (security by design) en verantwoording over besluitvorming rondom informatiebeveiliging nodig. Dit hoofdstuk waarborgt de rollen en verantwoordelijkheden op het gebied van informatiebeveiliging en benadrukt de (eind)verantwoordelijkheid van de lijnorganisatie. Er wordt beschreven hoe de principes en doelstellingen in dit informatiebeveiligingsbeleid worden geborgd en hoe de relevante wet- en regelgeving wordt geïmplementeerd en gehandhaafd.

5.1 Verantwoordelijkheden

5.1.1 Lijnverantwoordelijkheid
De Baseline Informatiebeveiliging Overheid (BIO) stelt dat informatiebeveiliging in de eerste plaats een lijnverantwoordelijkheid is. Dit betekent dat iedere lijnmanager verantwoordelijk is voor de beveiliging van de informatie binnen zijn processen, ketens en applicaties/systemen. De bestuurders en directie dragen daarbij de eindverantwoordelijkheid voor de naleving van informatiebeveiliging binnen de organisatie, in lijn met de verplichtingen uit de BIO en de NIS2-richtlijn.

Het is aan de lijnmanager om – eventueel met ondersteuning van CISO, ISO en FG – te bepalen:

- welke informatie als vertrouwelijk moet worden aangemerkt,(*Data classificatie*).
- welke risico's gepaard gaan met de verwerking van deze informatie, en (*Risicomanagement*).
- welke maatregelen passend en proportioneel zijn om deze risico's te beperken.(*Opvolging CISO en FG adviezen*).

Voor ieder gemeentelijk proces, applicatie en systeem wordt centraal vastgelegd welke lijnmanager als proceseigenaar optreedt en daarmee verantwoordelijk is voor de informatiebeveiliging. Voor processen waarin persoonsgegevens of bedrijfsgevoelige informatie worden verwerkt, wordt gebruikgemaakt van de bestaande registraties, zoals het verwerkingsregister en het overzicht van de bedrijfskritische processen, waarin de verantwoordelijken reeds zijn benoemd. Deze gegevens worden geïntegreerd in het ISMS, zodat één centrale en actuele basis ontstaat.

Wanneer er (nog) geen proceseigenaar is aangewezen, draagt de directie deze verantwoordelijkheid expliciet op aan een lijnmanager. Daarmee is gewaarborgd dat verantwoordelijkheden altijd helder en ondubbelzinnig zijn belegd.

Wanneer een lijnmanager taken laat uitvoeren door een andere organisatie, zoals een leverancier, shared service center of ketenpartner, blijft hij verantwoordelijk voor de waarborging van de belangen van de gemeenten en BWB. Dit wordt vastgelegd in een schriftelijke overeenkomst, zoals een dienstverleningsovereenkomst, verwerkersovereenkomst of gegevensleveringsovereenkomst. In lijn met de BIO en NIS2 dient de lijnmanager niet alleen te zorgen dat afspraken contractueel zijn vastgelegd, maar ook dat deze in de praktijk worden nageleefd. Dit vereist periodieke toetsing en monitoring van de dienstverlening en de getroffen beveiligingsmaatregelen. (*leverancier management en contractbeheer*).

Externe organisaties die geen onderdeel zijn van de overheid vallen niet rechtstreeks onder de BIO. In die gevallen bepaalt de opdrachtgever samen met de CISO welke informatiebeveiligingseisen van

toepassing zijn. Deze eisen moeten expliciet in het contract met de externe partij worden opgenomen en periodiek worden getoetst op naleving. (*inkoopbeleid*).

5.1.2 Ketenverantwoordelijkheid

De verschillende informatiesystemen in onze organisatie zijn onderling afhankelijk en ondersteunen samen een proces of keten. Om deze reden wijst de directie voor iedere keten één lijnmanager aan als proceseigenaar. Deze proceseigenaar is verantwoordelijk voor de beveiliging van de keten en stelt, op basis van een risicoanalyse, het vereiste beveiligingsniveau vast. Daarbij houdt hij rekening met specifieke afspraken en afhankelijkheden binnen de keten.

Het directieteam van de gemeente en/of BWB draagt de eindverantwoordelijkheid voor de borging van informatiebeveiliging en ziet erop toe dat er een actueel overzicht beschikbaar is van de ketens waar de gemeente(n) of de BWB deel van uitmaakt. In dit overzicht zijn de verantwoordelijkheden en afspraken met ketenpartners expliciet vastgelegd en wordt periodiek gecontroleerd of deze afspraken in de praktijk worden nageleefd.

Voorbeelden van ketensamenwerkingen en afhankelijkheden voor gemeenten zijn:
- Samenwerkingen in het Sociaal Domein, waarin de gemeente samenwerkt met zorgaanbieders, in het kader van Wmo- en jeugdzorgvoorzieningen.
- Het verkiezingsproces, waarbij gemeenten samenwerken met de Kiesraad en leveranciers van verkiezingssoftware en -systemen.
- De digitale toegangsketen, zoals DigiD en eHerkenning, waarbij gemeenten afhankelijk zijn van landelijke voorzieningen en leveranciers van authenticatiediensten.

5.1.3 Samenwerkingsverbanden

Gemeenten Culemborg, Tiel en West Betuwe nemen deel aan diverse samenwerkingsverbanden. De informatiebeveiliging binnen deze verbanden is doorgaans afhankelijk van meerdere partijen, wat de borging van beleid en maatregelen complexer maakt. Wanneer de gemeente of BWB binnen een samenwerkingsverband de grootste verantwoordelijkheid draagt – bijvoorbeeld bij het beheer van een gezamenlijke informatievoorziening – is dit beleid leidend.

5.2 Interne rollen en verantwoordelijkheden

Hieronder worden de rollen opgesomd die bijdragen aan het proces van informatiebeveiliging binnen de gemeente Culemborg, Tiel, West Betuwe en/of BWB. Basis voor de rolverdeling en de verdeling van de verantwoordelijkheden zijn de BIO en geldende wet- en regelgeving. De rollen en verantwoordelijkheden bij een cybercrisis worden apart beschreven in continuïteitsplanen.

5.2.1 De gemeenteraad

De gemeenteraad heeft binnen de eigen gemeente een toezichthoudende rol, gebaseerd op de controlerende taak die de Gemeentewet aan de raad toekent. De raad is bevoegd om het beleid en de uitvoering daarvan te controleren en te toetsen, waaronder het beleid op het gebied van informatiebeveiliging.

Daarnaast heeft de gemeenteraad een voorbeeldfunctie in het naleven en uitdragen van dit beleid en de bijbehorende tactische en operationele beleidsstukken.

5.2.2 College van burgemeester en wethouders

Het college van burgemeester en wethouders is bestuurlijk eindverantwoordelijk voor het organiseren van een passend niveau van informatiebeveiliging binnen de eigen organisatie. Het college stelt met dit beleidsdocument de kaders vast ten aanzien van informatiebeveiliging. Binnen het college is een portefeuillehouder informatiebeveiliging aangewezen.

Voor specifieke onderwerpen geldt een afwijkende bevoegdheidsverdeling. Zo is bij wet bepaald dat voor reisdocumenten de bevoegdheid tot het vaststellen van kaders niet bij het college, maar bij de burgemeester ligt.

Net als de gemeenteraad heeft ook het college een voorbeeldfunctie bij het naleven en uitdragen van dit beleid en de bijbehorende tactische en operationele beleidsstukken.

5.2.3 Gemeentesecretaris / directeur BWB

De gemeentesecretaris is ambtelijk eindverantwoordelijk voor de kaderstelling en sturing op tactisch niveau, alsmede voor de implementatie, borging en uitvoering van het informatiebeveiligingsbeleid binnen de organisatie. De gemeentesecretaris heeft de verantwoordelijkheid voor informatiebeveiliging gedelegeerd aan de directie, die zorgdraagt voor de feitelijke uitvoering en naleving.

5.2.4 Concern Controller
De Concern Controller van de gemeente heeft een brede inhoudelijk adviserende en signalerende taak voor wat betreft de samenhang van beleid, organisatie en middelen en het behalen van de bestuurlijke doelen. Hij is onafhankelijk en heeft tot taak als mee- en tegendenker te fungeren ten opzichte van de directie, is verantwoordelijk voor de opzet en voortdurende werking van een adequaat functionerend instrumentarium van planning en control met als resultaat relevante en integrale bestuurlijke informatievoorziening op basis waarvan de directie in control is. Daarnaast is de Concern Controller verantwoordelijk voor de totstandkoming en de handhaving van de financiële kaders, conform de Gemeentewet. Dit betreft de inrichting van de financiële organisatie, het financiële beheer en de uitgangspunten van het financieel beleid.

5.2.5 Lijnmanager
In de Baseline Informatiebeveiliging Overheid (BIO) is vastgelegd dat informatiebeveiliging een lijnverantwoordelijkheid is. Een andere benaming voor de lijnmanager is de proceseigenaar. Binnen onze organisatie zijn dit meestal de afdelings- teammanagers of teamleiders. Elke lijnmanager is eindverantwoordelijk voor een adequate beveiliging van de informatie in de processen, ketens en applicaties/systemen binnen zijn beheer. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Om deze verantwoordelijkheid waar te maken, dienen lijnmanagers goed ondersteund te worden.

5.2.6 Chief Information Security Officer (CISO)
De Chief Information Security Officer (CISO) vervult een strategische en toezichthoudende rol binnen de organisatie. Hij of zij adviseert en ondersteunt het lijnmanagement, de directie en het bestuur bij hun verantwoordelijkheid voor informatiebeveiliging, waaronder de implementatie en naleving van de Cyberbeveiligingswet. De CISO ziet daarbij toe op de werking en effectiviteit van maatregelen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie en persoonsgegevens borgen. Het advies van de CISO weegt zwaar mee in besluitvorming. Tot de taken behoren het actualiseren van het strategisch informatiebeveiligingsbeleid, de coördinatie van de uitvoering en de organisatie van toezicht en audits. De voortgang en bevindingen rapporteert de CISO rechtstreeks aan directie en bestuur. Daarnaast fungeert de CISO als centraal aanspreekpunt voor interne medewerkers en externe partijen, waaronder inwoners, samenwerkingspartners, de VNG, provincie, regio en ministeries. De CISO opereert onafhankelijk en is zodanig gepositioneerd dat hij of zij niet hiërarchisch onder het lijnmanagement valt. Hiermee worden de onafhankelijkheid en objectiviteit van toezicht en advisering gewaarborgd.

5.2.7 Information Security Officer (ISO)
De ISO ondersteunt de CISO en de lijnmanagers bij de uitvoering van het informatiebeveiligingsbeleid. De ISO is organisatiebreed verantwoordelijk voor advisering en ondersteuning op tactisch en operationeel niveau.
De ISO draagt bij aan het opstellen en actualiseren van procedures en beleid, adviseert bij de implementatie en uitvoering daarvan en ondersteunt bij projecten waarin informatiebeveiliging een rol speelt. Daarnaast houdt de ISO zich bezig met het uitvoeren van risicomanagement en met de implementatie en het beheer van het Information Security Management System (ISMS).

5.2.8 Beveiligingsbeheerder
De beveiligingsbeheerder is verantwoordelijk voor beheer en coördinatie op het gebied van informatiebeveiliging binnen een specifiek domein.
Er zijn zowel centrale beveiligingsbeheerders met een organisatiebrede scope, als decentrale beveiligingsbeheerders binnen afdelingen, teams of processen die toezien op naleving van specifieke wet- en regelgeving. Voorbeelden hiervan zijn de Beveiligingsfunctionaris BRP, de Beveiligingsfunctionaris Reisdocumenten en de Security Officer Suwinet.
Beveiligingsbeheerders werken nauw samen met de CISO en de ENSIA-coördinator om de aansluiting met het organisatiebrede beleid te waarborgen en de ENSIA-verantwoording volledig en juist uit te voeren.

5.2.9 ENSIA-Coördinator
De ENSIA-coördinator organiseert en coördineert het jaarlijkse ENSIA-verantwoordingsproces. Dit omvat het uitzetten van vragenlijsten, het verzamelen van bewijslast, de afstemming met betrokkenen en het bewaken van planning en kwaliteit. Daarbij ondersteunt de coördinator de CISO en lijnmanagers bij het aanleveren van de benodigde informatie.

De ENSIA-coördinator bereidt de rapportage voor richting het college van B&W, de gemeenteraad en de landelijke toezichthouders. De formele vaststelling en indiening hiervan ligt bij het college van B&W. Hoewel de CISO en de ENSIA-coördinator verschillende rollen hebben, werken zij nauw samen om ervoor te zorgen dat de ENSIA-verantwoording inhoudelijk juist, volledig en tijdig wordt opgeleverd.

5.2.10 Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) is een onafhankelijke toezichthouder die binnen de organisatie verantwoordelijk is voor het toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en overige relevante privacywetgeving. De FG adviseert bestuur, directie en organisatie over privacyvraagstukken, voert toezicht en controles uit, en fungeert als onafhankelijk aanspreekpunt voor zowel interne medewerkers als externe betrokkenen (zoals inwoners) en voor de Autoriteit Persoonsgegevens.

5.2.11 Privacy Officer
De Privacy Officer vervult een adviserende en coördinerende rol richting de organisatie op het gebied van privacybescherming. De Privacy Officer kan zelfstandig privacyrisico's binnen de organisatie signaleren en hierover proactief in gesprek gaan om passende adviezen te formuleren. Daarnaast voorziet de Privacy Officer zowel de Functionaris Gegevensbescherming (FG) als de CISO van relevante informatie over geïdentificeerde risico's en over de borging van privacy binnen de gehele organisatie.

5.3 Externe partijen

5.3.1 Externe Dienstverlener
Met alle leveranciers die in de vorm van (kantoor)automatisering, applicaties, IT-componenten en/of operationele technologie informatie van onze organisaties verwerken of operationele processen ondersteunen, worden afspraken gemaakt over de wijze waarop zij de informatiebeveiliging hebben geborgd. Deze leveranciers leggen hierover periodiek, conform de gemaakte afspraken, verantwoording af aan de proceseigenaar.

5.3.2 Rekenkamercommissie
De rekenkamercommissie ondersteunt de gemeenteraad bij zijn controlerende taken door onderzoek te doen naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het gemeentelijk beleid. De rekenkamercommissie kan zelfstandig een onderzoek (laten) uitvoeren naar de informatiebeveiliging van onze organisatie en rapporteert hierover aan de gemeenteraad.

5.3.3 Externe partij in een samenwerkingsverband
Externe partijen in een samenwerkingsverband, zoals ketenpartners of gemeenschappelijke regelingen, zijn verantwoordelijk voor de beveiliging van de gegevens die zij namens de gemeenten verwerken. Publieke partijen zijn verplicht zich te houden aan de Baseline Informatiebeveiliging Overheid (BIO). Private partijen zijn niet direct gebonden aan de BIO en dienen daarom via een schriftelijke overeenkomst, zoals een dienstverleningsovereenkomst, verwerkersovereenkomst of gegevensleveringsovereenkomst aan de overeengekomen beveiligingsvereisten te voldoen. Conform de NIS2-richtlijn en de Cyberbeveiligingswet ziet de gemeente er daarnaast op toe dat deze afspraken periodiek worden getoetst en nageleefd.

De gemeente en BWB blijven te allen tijde eindverantwoordelijk voor de informatiebeveiliging en de bescherming van (persoons)gegevens.

5.3.4 Externe Auditor
Een externe auditor is een partij die in opdracht van de gemeente maar volledig onder eigen verantwoording een onderzoek uitvoert of binnen een gestelde scope de organisatie voldoet aan gestelde normenkaders. Vanwege het ontbreken van een interne 3e lijn (op het gebied van informatiebeveiliging) volgens het Three Lines of Defence model is deze externe auditor de 3e lijns controle.

5.3.5 Informatiebeveiligingsdienst voor Gemeenten (VNG/IBD)
De IBD[2] is een onderdeel van de Vereniging Nederlandse Gemeenten (VNG) en levert ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. Gemeenten Culemborg, Tiel, West Betuwe en BWB maken gebruik van deze ondersteuning. De IBD informeert ons via vastgestelde contactpersonen namelijk de CISO en de algemeen contactpersoon informatiebeveiliging (ACIB)[3] en de vertrouwde contactpersoon informatiebeveiliging (VCIB)[4] .

2) De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).

3) Algemene waarschuwingen en informatie met een niet vertrouwelijk karakter

4) Informatie die vertrouwelijk is van karakter

6. Contactmomenten

Binnen de gemeente zijn er structurele contactmomenten in relatie tot informatiebeveiliging. Onderstaande tabel geeft een inzicht in deze momenten.

Contactmoment	Deelnemers	Frequentie	Doel
Portefeuillehouder overleg	Bestuurlijk opdrachtgever, ambtelijk opdrachtgever, CISO	Jaarlijks of indien nodig of gewenst	Informeren bestuurlijk opdrachtgever
Directie overleg	Directie en CISO	Ieder halfjaar	Bespreken van de kwartaalrapportage informatiebeveiliging kwetsbaarheden en incidenten
Informatie beveiliging en bedrijfsvoering	CISO, Directeuren bedrijfsvoering 3 gemeenten en BWB	Ieder halfjaar en indien nodig of gewenst	Afstemming en risicoafweging tussen informatiebeveiliging in relatie tot de bedrijfsvoering
Bilateraal overleg	CISO, Directeur BWB	2-wekelijks	Afstemming, advies en regie op informatieveiligheid
Security overleg	CISO, ISO en ICT coördinator	2-wekelijks	Afstemming en coördinatie van informatieveiligheid en ICT
Afstemmingsoverleg	CISO, Informatiemanager, Informatiebeheer, changemanager en portfoliomanager	2-wekelijks	Afstemming en coördinatie van informatieveiligheid en Informatiemanagement, ICT en projecten
Compliance overleg	CISO, FG en Privacy officers 3 gemeenten en BWB	2-wekelijks	Afstemming en coördinatie van informatieveiligheid en privacy
ENSIA-verantwoording	Proces eigenaren, procesbetrokkenen, ENSIA coördinator, CISO, ISO's, beveiligingsbeheerders en privacy adviseur(s)	Eindverantwoording in maart, tussenrapportage in oktober (jaarlijks)	In beeld stand van zaken implementatie informatiebeveiliging ENSIA-onderdelen. input voor bestuurlijke rapportage aan interne en externe toezichthouders, jaarverslag en Raadsinformatiebrief
Informatiebeveiliging crisisoverleg* *Dit is via het Business Continuïteit Management (BCM) Proces en cyberweerbaarheidsplan georganiseerd	Directeur bedrijfsvoering, CISO, Incident manager, communicatiemedewerker, privacy officer, proces eigenaar voor het domein waar de crisis betrekking op heeft	Op afroep bij grote incidenten	Ondervangen en grip krijgen op een crisis input voor analyse en rapportage van incident

7. Rapportagemomenten informatiebeveiliging

7.1 Periodieke rapportages

Periodieke rapportages vloeien voort uit bovengenoemde contactmomenten met stakeholders. Rapportages worden opgesteld van incidenten, het verantwoordingstraject ENSIA en periodieke rapportages over de stand van zaken van de implementatie van informatiebeveiliging. Aangezien het college en de Raad met name een rol spelen in het verantwoordingstraject ENSIA wordt dit traject in onderstaande paragraaf toegelicht. In het informatiebeveiligingsplan is een detailplanning opgenomen van dit verantwoordingstraject.

7.2 Verantwoordingstraject ENSIA

Ter afsluiting van het jaarlijkse verantwoordingstraject[5] rapporteren lijnmanagers over de stand van zaken met betrekking tot informatiebeveiliging binnen hun bedrijfsprocessen van het afgelopen jaar. De ENSIA-coördinator coördineert dit proces en stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de lijnmanagers/proceseigenaren een bestuurlijke rapportage op voor de ambtelijke en bestuurlijke opdrachtgever.

5) Verantwoording vindt plaats via de landelijk voorgeschreven systematiek ENSIA (Eenduidige Normatiek Single Information Audit)

Het college van B&W legt met deze bestuurlijke rapportage, een raadsinformatiebrief én met een aparte paragraaf in het jaarverslag verantwoording af aan zijn interne toezichthouder (de gemeenteraad) én aan de externe toezichthouders (Rijk). Op deze wijze kan de ambtelijk en de bestuurlijk opdrachtgever en het college sturen op informatiebeveiliging. Zij kunnen hiermee besluiten nemen om informatiebeveiligingsrisico's tot een acceptabel niveau te brengen.

8. Afkortingen en begrippenlijst

AP	Autoriteit Persoonsgegevens; Nederlandse Toezichthouder in het kader van de AVG en bescherming van persoonsgegevens.
AVG	Algemene Verordening Gegevensbescherming; De AVG is een Europese Verordening met als doel om natuurlijke personen en de verwerking van hun persoonsgegevens te beschermen.
BIO	Baseline Informatiebeveiliging Overheid; Het normenkader voor de Nederlandse overheid om de weerbaarheid op het gebied van informatieveiligheid te waarborgen.
B&W	Burgemeester en Wethouders; Het college van burgemeester en wethouders vormt het dagelijks bestuur van een gemeente.
CBW	Cyberbeveiligingswet; Landelijke wetgeving die regelt dat met name essentiële organisaties in Nederland voldoende informatiebeveiligingsmaatregelen nemen om de weerbaarheid te versterken.
CISO	Chief Information Security Officer; Dit is de organisatiebreed georiënteerde functionaris die verantwoordelijk is voor het maken, uitdragen van het informatiebeveiligingsbeleid. De CISO heeft een onafhankelijke positie binnen de organisatie en mag gevraagd en ongevraagd adviseren richting directie en bestuur over informatieveiligheid aspecten. Vanuit de BIO is het aanstellen van een CISO een verplichte overheidsmaatregel.
ENSIA	Eenduidige Normatiek Single Information Audit. Gemeenten zijn verplicht om volgens de ENSIA-methodiek verantwoording af te leggen over de stand van zaken met betrekking tot informatieveiligheid binnen de organisatie. Dit gaat zowel horizontaal (naar het eigen bestuur) als verticaal naar de landelijke toezichthouders.
FG	Functionaris Gegevensbescherming: Functionaris die binnen organisaties verantwoordelijk is voor het toezicht houden op de juiste verwerking van persoonsgegevens en het borgen van de privacy van inwoners en medewerkers.
IBD	Informatie Beveiligings Dienst. De IBD ondersteunt specifiek gemeenten bij het werken aan weerbaarheid op het gebied van informatiebeveiliging. Hierin zit ook incidentbeheer en incidentpreventie.
ICT	Informatie- en Communicatie Technologie
ISMS	Information Security Management System. Het is een samenhangend stelsel van beleid, processen, procedures en maatregelen waarmee een organisatie informatiebeveiliging systematisch beheert, borgt en continu verbetert. (PDCA)
IOT	Het Internet of Things, (in het Nederlands het Internet der Dingen), verwijst naar het geheel van slimme apparaten die zijn verbonden met het internet.
I&A	Informatisering en Automatisering, een samenhang van de digitale informatievoorziening (techniek en gegevens).
Keten	Een keten wordt binnen de overheid gedefinieerd als "het samenhangende geheel van processen, informatiesystemen en organisaties die gezamenlijk verantwoordelijk zijn voor de levering van een dienst of voorziening aan burgers, bedrijven of instellingen" (NORA)
NCSC	Het Nationaal Cyber Security Centrum is een organisatie die de weerbaarheid van de Nederlandse samenleving in het digitale domein tracht te vergroten.
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid is een instantie van de Nederlandse overheid die is ingesteld om Nederland te beschermen tegen bedreigingen die de maatschappij kunnen ontwrichten
NEN-ISO 27001/27002	Internationale norm en format voor Informatiebeveiliging, uitgegeven door het Nederlands Normalisatie Instituut (NEN) en de Internationale Standaardisatie Organisatie (ISO); voorheen bekend als Code voor Informatiebeveiliging.
NIS2	De Network and Information Security Directive (NIS2-richtlijn) is eind 2022 vastgesteld door de Europese Unie. De richtlijn is gericht op een versterking van de digitale en eco-

	nomische weerbaarheid van Europese lidstaten en wordt op dit moment omgezet naar de Nederlandse Cyberbeveiligingswet.
RDI	Rijksinspectie Digitale Infrastructuur (RDI) en samenwerking, Binnen het ministerie van Justitie en Veiligheid werkt de Rijksinspectie Digitale Infrastructuur (RDI) nauw samen met andere toezichthouders. Zij participeren in het overleg STD W (Samenwerkend Toezicht Digitale Weerbaarheid) dat toezicht coördineert op vitale processen. Toezichthouder Cbw en NIS2.
WPG	De Wet politiegegevens (Wpg) is een Nederlandse wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens.