Gemeente Nuenen

GEMEENTEBLAD

Officiële uitgave van de gemeente Nuenen, Gerwen en Nederwetten

Nr. 542704

16 december 2025

Strategisch Informatie Beveiligheidsbeleid Dommelvallei Organisaties 2025-2029

1 Visie en missie op informatieveiligheid

Gemeenten wisselen op alle beleidsterreinen informatie uit. Gemeenten willen hierbij een betrouwbare partner zijn voor inwoners, medewerkers en zakelijke partners en hebben hierbij een maatschappelijke en wettelijke verantwoordelijkheid. Door informatie te delen kunnen gemeenten de dienstverlening beter organiseren en de veiligheid van inwoners waarborgen.

1.1 Missie

De gemeenten Nuenen, Son en Breugel en Geldrop-Mierlo werken samen om hun eigen en gezamenlijke maatschappelijke opgaven en bestuurlijke ambities te realiseren. Technologische ontwikkelingen, digitalisering en toepassingen van kunstmatige intelligentie kunnen bijdragen aan deze opgaven. Deze opgaves en ontwikkelingen kunnen alleen succesvol zijn in een veilige en betrouwbare omgeving. De gemeenten nemen deel in de gemeenschappelijke regeling Dienst Dommelvallei.

De Dommelvallei-organisaties staan gezamenlijk voor een daadkrachtige, verbindende en betrouwbare organisatie: “Een toekomstbestendige bedrijfsvoering en dienstverlening, die bijdraagt aan een weerbare en wendbare organisatie”. Om dit te helpen realiseren en versterken zijn verdere informatisering en digitalisering cruciaal. Het borgen van de informatieveiligheid is hierbij een belangrijke randvoorwaarde.

1.2 Visie

De vier organisaties werken samen op basis van een krachtig zakelijk partnerschap, gedreven door wederkerigheid en collectieve doelstellingen. ‘Van, voor en door’, als credo onder het samenspel tussen de vier partnerorganisaties.

De gemeenten blijven eindverantwoordelijk voor de informatiebeveiliging. Zij hebben een aantal uitvoeringstaken belegd bij Dienst Dommelvallei. Dienst Dommelvallei is de organisatie die verantwoordelijk is voor een toekomstbestendige uitvoering van de bedrijfsvoeringstaken: Personeel & Organisatie en Kwaliteit & Control, Informatisering en Automatisering en Financiën. Voor de gemeenten Nuenen en Son en Breugel verricht Dienst Dommelvallei tevens taken op gebied van Klantcontactcentrum/ Burgerzaken en Werk & Inkomen. Hiermee bedient Dienst Dommelvallei in totaal circa 83.000 inwoners en 1.000 interne en externe medewerkers (ca 650 fte). Dienst Dommelvallei zet hierbij in op innovaties om de kwaliteit en doelmatigheid van haar dienstverlening hoog te houden én om te anticiperen op de (krappe) arbeidsmarkt.

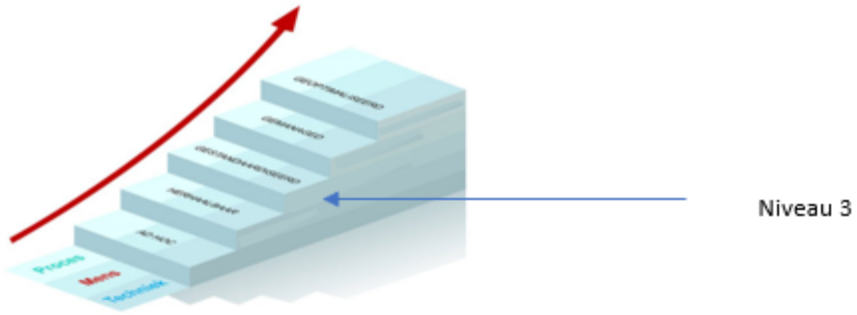
1.3 Samenhang tussen Missie, Visie en informatieveiligheid

Om de kansen te nemen en een toekomstbestendige bedrijfsvoering en dienstverlening te realiseren, waarbij ingezet wordt op innovatie, klantgerichtheid, flexibiliteit en weerbaarheid, is het nodig om op het gebied van informatieveiligheid de basis op orde hebben. Met de basis op orde is informatieveiligheid geborgd binnen de gemeentelijke processen en er wordt voldaan aan wet- en regelgeving. Medewerkers en hun ketenpartners, zoals bijvoorbeeld samenwerkingsverbanden binnen het Sociaal Domein, moeten kunnen beschikken over betrouwbare informatie om de inwoners en bedrijven optimaal te kunnen helpen en adviseren. Bovendien moeten inwoners en medewerkers er op kunnen vertrouwen dat hun gegevens in goede handen zijn. Het is daarom belangrijk dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie binnen de processen zijn geborgd. De Dommelvallei-organisaties volgen hierbij de landelijke Baseline Informatiebeveiliging Overheid (BIO) die kaders en richting geeft. De Dommelvallei-organisaties weten op deze wijze risico’s te verkleinen tot een acceptabel niveau in lijn met de gestelde ambities.

1.4 Ambitieniveau informatieveiligheid

De door de Dommelvallei organisaties vastgestelde ambitie is om te groeien naar een minimaal landelijk vereist volwassenheidsniveau 3. Hiermee hebben zij beheersingsmaatregelen gedocumenteerd en worden deze beheersmaatregelen op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. Zodra dat niveau bereikt is, hebben de Dommelvallei-organisaties informatieveiligheid geborgd binnen de processen en kunnen aantoonbaar maken richting medewerkers en inwoners dat informatiebeveiliging is geborgd. Zij voldoen hiermee aan wet- en regelgeving.

De Basis op Orde, dat is de ambitie.



Figuur: volwassenheidsmodel informatiebeveiliging Norea schaal 1 tot en met 5[1].

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 met digitalisering meekomen. Kwetsbaarheden en dreigingen nemen in het digitale domein toe. Landelijk presenteren het Nationaal Cyber Security Center (NCSC[2]), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV[3]) 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 de Dommelvallei-organisaties relevant zijn. Ook uit onze eigen monitoring blijken kwetsbaarheden en dreigingen toe te nemen. Dit vraagt om continue extra inspanningen om de digitale weerbaarheid te versterken en te borgen.

De Dommelvallei-organisaties staan gezamenlijk voor een daadkrachtige, verbindende en betrouwbare organisatie: "Een toekomstgerichte informatievoorziening, die bijdraagt aan een weerbare en wendbare organisatie". Het borgen van de informatieveiligheid is hierbij een belangrijke randvoorwaarde.

Dit beleid geldt voor de jaren 2025 tot en met 2029 en vervangt het "Strategisch Gemeentelijk Informatiebeveiligingsbeleid Dommelvallei-organisaties 2020 tot en met 2025".

2.1 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 (persoons)gegevens en andere informatie.

De primaire doelstelling van informatiebeveiliging is door middel van een risico gebaseerde aanpak, informatiebeveiliging op een aantoonbare wijze te beheersen. Hiertoe moet een managementsysteem oftewel een Information Security Management System (ISMS) voor informatiebeveiliging worden ingericht, geïmplementeerd, onderhouden en continue verbeterd. Het managementsysteem voor informatiebeveiliging moet o.a. bevatten de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van het managementsysteem van informatiebeveiliging (bijv. procedures, standaarden en werkinstructies). Deze aanpak draagt bij aan het realiseren van een moderne en veilige informatievoorziening en een effectief besturingsmodel.

Informatiebeveiliging gaat over organisatorische, fysieke en digitale aspecten. Daarnaast is de mens onze belangrijkste schakel in het geheel. Om weerbaarder te worden en dit ook te blijven moet continu gewerkt worden aan het versterken van al deze aspecten. "Informatieveiligheid is een bestuurlijke verantwoordelijkheid".

1) Volwassenheidsmodel informatiebeveiliging (nba.nl)
2) Het Nationaal Cyber Security Centrum is een organisatie die de weerbaarheid van de Nederlandse samenleving in het digitale domein tracht te vergroten.
3) 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

Informatiebeveiliging is geen doel op zichzelf, maar moet in verhouding worden bekeken tot de doelstellingen die de Dommelvallei-organisaties hebben en de werkzaamheden die vereist zijn om die doelstellingen uit te kunnen voeren. Het geschreven informatiebeveiligingsbeleid vraagt om continue bewuste risico-afwegingen en het nemen van besluiten om deze risico's te verkleinen.

2.2 Doel en reikwijdte van dit beleid
Dit strategisch informatiebeveiligingsbeleid 2025-2029 is het bestuurlijk kader om informatie te beschermen, zodat de Dommelvallei-organisaties voldoen aan relevante wet- en regelgeving. Dit beleid draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan een toekomstbestendige bedrijfsvoering en dienstverlening en het behalen van overige 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 strategische informatiebeveiligingsbeleid is zoals in paragraaf 2.1 vermeld, gericht op het inrichten, implementeren, onderhouden en continue verbeteren van een managementsysteem voor informatiebeveiliging.

Dit beleid is van toepassing op alle Dommelvallei-organisaties, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en voor dit onderdeel betrokken externe partijen, 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 bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatievoorziening 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 Dommelvallei-organisaties worden gebruikt en waarvan de Dommelvallei-organisaties eigenaar zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen is dit beveiligingsbeleid ook van toepassing[4].

De Dommelvallei-organisaties hebben voor privacy elk een apart beleid opgesteld en privacybeleid valt hiermee buiten de scope van dit informatiebeveiligingsbeleid.

2.3 Eigenaarschap en evaluatie van dit beleid

2.3.1 Gemeenten
Het college van B&W is verantwoordelijk voor:
- Beleidsbepaling, stelt dit beleid vast, draagt het uit en houdt toezicht op de naleving door het management.
- Het toewijzen van voldoende middelen en het ondersteunen van de implementatie en naleving van dit beleid.

2.3.2 Dienst Dommelvallei
Het Bestuur is verantwoordelijk voor:
- Beleidsbepaling, stelt dit beleid vast, draagt het uit en houdt toezicht op de naleving door het management.
- Het toewijzen van voldoende middelen en het ondersteunen van de implementatie en naleving van dit beleid.

De Chief Information Security Officer (CISO) is beheerder van dit document en zal dit Informatiebeveiligingsbeleid periodiek evalueren en indien nodig aanpassen aan veranderde inzichten. Indien sprake is van significante wijzingen, zal het opnieuw ter vaststelling worden voorgelegd.

2.4 Communicatie van dit beleid
Na vaststelling van dit beleid wordt dit beleid gepubliceerd en via het (lijn)management gecommuniceerd met bestuurders, medewerkers en relevante externe partijen. Daarnaast zullen stakeholders via bewustwordingsactiviteiten worden meegenomen waarom informatiebeveiliging voor hen van belang is.

4) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf

2.5 Leeswijzer
In hoofdstuk 3 wordt het beleidskader van het strategisch beleid uiteengezet en de uitgangspunten en randvoorwaarden om dit beleid te implementeren. Hoofdstuk 4 geeft inzicht in actuele ontwikkelingen. In hoofdstuk 5 staat de organisatie van informatiebeveiliging opgenomen en in hoofdstuk 6 de overlegstructuur met stakeholders. Tot slot in hoofdstuk 7 de rapportagemomenten.

3 Beleidskader Informatieveiligheid
3.1 Plaats van dit beleid
Het strategisch informatiebeveiligingsbeleid is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het strategisch informatiebeveiligingsbeleid is een onderdeel van het informatiebeleid[5] en bestaat uit de volgende documenten:
1. het document dat u nu leest;
2. tactische informatiebeveiligingsbeleid, specifieke (tactische) beleidsdocumenten;
3. operationele informatiebeveiligingsplan(nen), procesbeschrijvingen en werkinstructies.

Aan de hand van onderstaande afbeelding wordt bovenstaande nader toegelicht.

Strategisch informatiebeveiligingsbeleid
Het strategische informatiebeveiligingsbeleid geeft kaders en richting om op het gebied van informatiebeveiliging weerbaarder te worden en dat ook te blijven.

Opgesteld door: CISO
Vastgesteld door: College B&W en Bestuur DDV

Tactisch informatiebeveiligingsbeleid
In het tactische informatiebeveiligingsbeleid staan onderwerp specifieke beleidsregels die de implementatie van informatiebeveiliging verder verplicht stelt en vorm geeft, zoals het beleid toegang tot digitale informatie, wachtwoordbeleid.

Opgesteld door: CISO
Vastgesteld door: Directie

Specifieke beleidskaders
Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen[6]. Hiervoor gelden specifieke beleidskaders zoals het Suwinetbeleid (Suwinet), het informatiebeveiligingsbeleid voor webapplicaties (Digitale identiteit: DigiD) en voor de basisregistratie personen (BRP) en reisdocumenten het beveiligingsbeleid BRP en reisdocumenten.

Opgesteld door: beleidsmedewerker bijvoorbeeld security officer Suwinet
Vastgesteld door: Directie

Operationele plannen, processen en instructies
De uitwerking van het strategische en het tactische beleid staat opgenomen in informatiebeveiligingsplan(nen). Deze plannen wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses. Het generieke informatiebeveiligingsplan is onderdeel van het informatieplan, thema "Veilig en Vertrouwd".

Opgesteld door: vakinhoudelijke collega's
Vastgesteld door: proceseigenaar

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) richtlijn aangenomen. In Nederland wordt deze richtlijn omgezet naar een landelijke Cyberbeveiligingswet. Gemeenten zijn, net als andere overheidsinstanties zoals waterschappen, onder de NIS2-implementatiewet, de Cyberbeveiligingswet, als essentiële entiteiten aangemerkt. Dit betekent dat digitale veiligheid een wettelijke verplichting is geworden.

In een notendop houdt de wet het volgende in:
- Naast het gebruikelijke toezicht achteraf, worden ook vooraf audits uitgevoerd op de digitale beveiliging van de gemeenten. Hiervoor is de Rijksinspectie Digitale Infrastructuur (RDI) aangesteld als toezichthouder.
- Gemeenten hebben een registratieplicht, een zorgplicht voor digitale veiligheid en een meldplicht voor significante (cyber)incidenten. Ook hebben zij recht op hulp bij digitale incidenten. De bepalingen zijn opgenomen in de Cyberbeveiligingswet.

5) Vormt de kaders en speerpunten voor het vormgeven van de informatiesamenleving door en in de gemeenten van de Dommelvallei
6) zoals Wet Basisregistratie Personen (BRP), Paspoortwet/ Reisdocumenten, Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), Digitale Identiteit (DigiD), Wet Basisregistratie Adressen en Gebouwen (BAG), Wet Basisregistratie Grootschalige Topografie (BGT), Wet Basisregistratie Ondergrond (BRO), Cybersecurity Implementatie Richtlijn, AI-act

Aangezien Dienst Dommelvallei taken uitvoert voor de gemeenten geldt deze wetgeving ook voor de Dienst.

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 de Dienst Dommelvallei-organisaties helpt om aan de Cyberbeveiligingswet te voldoen.

Dit strategische informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid BIO2. De BIO2 is als volgt opgebouwd:

- NEN-ISO/IEC 27001:2023[7]
- NEN-ISO/IEC 27002:2022
- een lijst met aanvullende overheidsmaatregelen

3.2.3 Cybersecurity Implementatie Richtlijn (CSIR)

Onze organisaties gebruiken de BIO als beveiligingsnorm voor kantoorautomatisering. Voor het beveiligen van procesautomatiseringssystemen bestaan aanvullende beveiligingseisen die niet in de BIO staan. Voor de bescherming van Proces Automatisering is 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

In de Cyberbeveiligingswet krijgt de bestuurder een nadrukkelijkere rol. Bestuurders dienen binnen twee jaar na inwerkingtreding van deze wet een opleiding te volgen op het gebied van informatieveiligheid.

De onderstaande 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op de cyberbeveiligingswet en gaan over de waarden die de bestuurder zichzelf oplegt. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers.

<u>De 10 principes zijn:</u>

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 staan nader uitgewerkt in de uitgewerkte rolverdeling van hoofdstuk 5, in het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

3.4 Uitgangspunten

Zoals hierboven toegelicht vormt het strategisch informatiebeveiligingsbeleid de basis voor het beschermen van de informatie en systemen binnen een organisatie. De belangrijkste uitgangspunten hiervan zijn:

3.4.1 Verantwoordelijkheid en betrokkenheid

- Het beleid benadrukt dat beveiliging een gezamenlijke verantwoordelijkheid is van alle medewerkers, van bestuur, management tot eindgebruikers.
- Het bestuur en management dragen dit beleid uit en sturen op de implementatie van dit beleid.

7) 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.

- 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 haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan dit beleid.
- Interne en externe communicatie relevant voor het managementsysteem wordt vastgesteld.

3.4.2 Risicogebaseerde aanpak
- Beveiligingsmaatregelen worden afgestemd op de risico's die de organisatie loopt, zodat de meest kritieke informatie en systemen prioriteit krijgen.
- Informatiebeveiliging is een onderdeel van risicomanagement. Risico's moeten in kaart gebracht worden en door de proceseigenaar worden afgewogen.
- De inrichting van informatiebeveiliging is proces-gestuurd en risicogebaseerd. De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Dit houdt in dat beheersmaatregelen volgens een voorgeschreven risicomanagement methodiek tot stand komen.
- Om te garanderen dat informatiebeveiligingsgegevens actueel, volledig en juist zijn wordt een aantal gegevens zoals risico's en incidenten centraal vastgelegd en periodiek geactualiseerd.

3.4.3 Integrale benadering
- Informatiebeveiliging wordt gezien als een onderdeel van de bredere bedrijfsstrategie en niet als een losstaand technisch aspect.

3.4.4 Continuïteit en veerkracht
- Het waarborgen van de bedrijfscontinuïteit door middel van preventie, detectie en herstelmaatregelen.
- De Dommelvallei-organisaties nemen maatregelen om de organisaties te beschermen tegen cyberdreigingen, om van incidenten te kunnen herstellen indien cyberdreigingen zich voordoen en de impact van de cyberdreiging te reduceren.
- De organisaties zijn cyberweerbaar doordat het (kritieke) processen identificeert en deze overeenkomstig beveiligt.
- Werkinstructies, procedures en beleid worden periodiek getest.

3.4.5 Wet- en regelgeving
- Naleving van relevante wet- en regelgeving, zoals de Cyberbeveiligingswet, wordt als uitgangspunt genomen.

3.4.6 Bewustwording, training en digitaal vaardig gedrag
- Medewerkers worden actief betrokken door middel van bewustwordingsprogramma's en training om beveiligingsbewustzijn te vergroten.
- Het management heeft continu aandacht voor het vergroten van digitaal vaardig gedrag van medewerkers om zo de menselijke schakel te versterken.
- Bestuurders en medewerkers dienen verantwoord om te gaan met (persoons)gegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Indien van toepassing voor het uitvoeren van werkzaamheden worden medewerkers getraind in het gebruik van beveiligingsprocedures.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Informatiebeveiliging maakt deel uit van de HR-gesprekscyclus en wordt besproken tussen de manager en de medewerker.

3.4.7 Duidelijke procedures en beleid
- Het vastleggen van heldere richtlijnen en procedures voor het omgaan met informatie en incidenten. Informatiebeveiligingsincidenten worden afgehandeld volgens een gestandaardiseerd proces.

3.4.8 Continue verbetering
- Het beleid is dynamisch en wordt regelmatig geëvalueerd en aangepast op basis van nieuwe risico's, technologische ontwikkelingen en ervaringen.

- Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én coördinatie wordt de kwaliteit van de informatievoorziening verankerd en verbeterd binnen de organisatie.
- Om het informatiebeveiligingsproces te structureren wordt gebruik gemaakt van een managementsysteem.
- Elk bedrijfsproces en informatiesysteem binnen scope van het managementsysteem (ISMS) is bekend.
- 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 van informatiebeveiliging (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging.
- Tijdens periodieke gesprekken met directie en management 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 gebruikt wordt, heeft een eigenaar (leidinggevende) die de waarde bepaalt van de informatie die het bevat. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie die verantwoording aflegt over de beveiliging hiervan.
- De rol van de coördinator van informatiebeveiliging (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.

3.4.9 Overige uitgangspunten

De verantwoordelijkheid voor informatiebeveiliging eindigt niet bij de poort van de Dommelvallei-organisaties. 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 wordt ingezet op het beschermen van informatie (data) ongeacht waar deze zich bevindt.

3.5 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:

1. Managementondersteuning: Topmanagement steunt actief en geeft prioriteit aan beveiliging.
2. Beschikbare middelen: Voldoende budget, personeel en technologieën zijn aanwezig.
3. Communicatie en training: Medewerkers, leidinggevenden en bestuur worden geïnformeerd en getraind over het beleid en hun rol bijvoorbeeld met bewustwordingsactiviteiten zoals risicoworkshops.
4. Organisatie en verantwoordelijkheden: Duidelijke rollen en verantwoordelijkheden worden vastgesteld.
5. Technische infrastructuur: De juiste beveiligingstechnologieën worden geïmplementeerd en onderhouden.
6. Cultuur en gedragsverandering: Een organisatiecultuur die beveiliging serieus neemt en alertheid stimuleert.
7. Monitoring en rapportage[8]: Systemen voor het meten van naleving en effectiviteit worden ingericht. De informatiebeveiligingseisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd door verantwoordelijken.
8. Wet- en regelgeving: Het beleid sluit aan bij en voldoet aan relevante wet- en regelgeving
9. Jaarlijks wordt het informatiebeveiligingsplan(roadmap) geactualiseerd onder aansturing van de CISO, gebaseerd op:
   a. dit informatiebeveiligingsbeleid;

8) *Informatiebeveiligingsbeleid - Intranet Dommelvallei-organisaties*

b. de uitkomsten van het jaarlijkse verantwoordingstraject Eenduidige Normatiek Single Information Audit (ENSIA[9]);
c. andere audit resultaten, zoals de (Financiële) Jaarrekening controle, WPG-audit;
d. het dreigingsbeeld gemeenten van de Informatiebeveiligingsdienst (IBD), National Cyber Security Centre (NCSC);
e. uitkomsten uitgevoerde risico-analyses

4 Ontwikkelingen

Hieronder zijn de ontwikkelingen beschreven die van belang zijn voor de actualisering van dit informatiebeveiligingsbeleid.

4.1 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Gemeenten worden geconfronteerd met een complex en structureel dreigingslandschap. Deze digitale dreigingen raken direct de continuïteit van gemeentelijke dienstverlening en het vertrouwen van inwoners.

De Informatiebeveiligingsdienst voor Gemeenten (IBD)[10] publiceert jaarlijks het Dreigbeeld Informatiebeveiliging Nederlandse Gemeenten. Het dreigbeeld geeft een actueel zicht op deze dreigingen, incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Het doel van dit dreigbeeld is om gemeenten inzicht te geven in de belangrijkste risico's op het gebied van informatiebeveiliging, zodat ze hun digitale weerbaarheid kunnen versterken. Het dreigbeeld helpt gemeenten om bewuster te worden van de dreigingen en kwetsbaarheden waarmee ze te maken kunnen krijgen, en om maatregelen te nemen om deze risico's te beperken.

Dit dreigingsbeeld is daarmee onderwerp van de risicoworkshops aan Directie en management om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

4.2 Informatie uit incidenten, inbreuken op de beveiliging

De Dommelvallei-organisaties kennen naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd en lering uit kan worden getrokken.

Voorgekomen incidenten zijn hiermee als input gebruikt bij het actualiseren van dit beleid.

5 Organisatie van informatiebeveiliging

Zoals eerder aangegeven hebben de Dommelvallei-organisaties een gezamenlijke verantwoordelijkheid voor de beveiliging van de 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 beschrijft welke rollen, taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. Het (lijn)management speelt een cruciale rol bij het uitvoeren van dit beleid. De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. Hieronder zijn de ambtelijke rollen in een illustratie weergegeven. Nadere toelichting volgt in de onderstaande paragrafen.

5.1 Interne rollen en verantwoordelijkheden

5.1.1 Gemeenteraad

De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeenteraad toekent. De Gemeenteraad is bevoegd voor de controle en toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging.

9) 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.

10) *Zie paragraaf 5.2.5*

5.1.2 College van B&W Gemeenten
Het College van Burgemeester en Wethouders is bestuurlijk verantwoordelijk voor een passend niveau van informatiebeveiliging in onze organisatie. Het college stelt het strategisch informatiebeveiligingsbeleid vast. De Burgemeester is portefeuillehouder voor informatiebeveiliging. Bij het onderwerp reisdocumenten is bij wet bepaald dat de bevoegdheid voor het vaststellen van kaders bij de burgemeester ligt in plaats van bij het college.

Het college van burgemeester en wethouders legt middels de zelfevaluatie Eenduidige Normatiek Single Information Audit (ENSIA) jaarlijks verantwoording af over informatiebeveiliging aan de raad en aan externe toezichthouders. Verder vindt er in het jaarverslag verantwoording plaats in de paragraaf over informatiebeveiliging.

De ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging is door het college gemandateerd aan de gemeentesecretaris van de gemeente.

5.1.3 Bestuur Dienst Dommelvallei
Het Bestuur Dienst Dommelvallei is bestuurlijk verantwoordelijk voor de borging van informatieveiligheid binnen Dienst Dommelvallei. Het Bestuur bestaat uit de burgemeesters van de drie gemeenten en van elke gemeente een wethouder. Zij stelt het strategisch beleid voor informatieveiligheid vast.

De ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging is door het Bestuur gemandateerd aan de directeur van Dienst Dommelvallei.

5.1.4 Directie
De directeur (Dienst Dommelvallei)/ gemeentesecretaris (gemeente) is ambtelijk verantwoordelijk voor kaderstelling en sturing op tactisch niveau, voor de implementatie, borging en uitvoering van het informatiebeveiligingsbeleid binnen de organisatie. De directeur stuurt hierbij op in beeld gebrachte concernrisico's. De directeuren van de organisaties vinden centrale en gezamenlijke afstemming via het Directieberaad.

5.1.4.1 Directieberaad
Het Directieberaad bestaat uit de gemeentesecretarissen van de gemeenten en de directeur van Dienst Dommelvallei. De gemeentesecretarissen adviseren hierbij de directeur van de Dienst bij inbreng van stukken aan het Bestuur. Het Directieberaad wordt op haar beurt weer geadviseerd door het opdrachtgever – opdrachtnemer overleg.

5.1.5 Ondernemingsraad (OR)
De ondernemingsraad (OR) komt op voor de belangen van het personeel in een onderneming of organisatie. De OR mag meedenken over bedrijfseconomische en sociale onderwerpen. De OR kan door advisering of instemming invloed hebben op de bedrijfsvoering zoals bij het tactisch beleid logging en monitoring.

5.1.5.1 Opdrachtgever- opdrachtnemer overleg (OGON)
Via het OGON waarin managers van de Dienstdommelvallei organisaties zitting hebben, vindt afstemming plaats over organisatiebrede organisationtwikkelingen, initiatieven, processen en projecten. Het OGON stuurt daarnaast op reguliere informatiebeveiligingswerkzaamheden. De managers bewaken via dit overleg de risico's binnen de processen en de harmonisatie tussen de organisaties onderling. Daarnaast bewaken zij de voortgang op de ENSIA en de doorontwikkelplannen binnen de Dommelvallei organisaties, bijvoorbeeld het doorontwikkelplan Suwinet. Het OGON adviseert Directie.

5.1.6 Business Controller
De Business Controller heeft een brede inhoudelijk adviserende en signalerende taak voor wat betreft de samenhang van informatiebeveiligingsbeleid, organisatie en middelen (BOM) en het behalen van de bestuurlijke doelen. Hij heeft een onafhankelijke taak ten opzichte van de directie.

5.1.7 Lijnmanager (proceseigenaren)
In de Baseline Informatiebeveiliging Overheid (BIO) is vastgelegd dat de borging van informatiebeveiliging een lijnverantwoordelijkheid is. Een andere benaming voor de lijnmanager is de proceseigenaar. 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 door een information security officer.

Lijnmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiliging beschermende activiteiten. Afstemming over de inhoudelijke aanpak vindt periodiek plaats door het onderwerp informatiebeveiliging (via managers bedrijfsvoering gemeenten, concernmanager en manager IV Dienst Dommelvallei) te bespreken in het OGON.

De lijnmanagers zorgen dat de inrichting van informatiebeveiliging voldoet aan de vereiste wet- en regelgeving die op hun processen van toepassing is en geven invulling aan de rollen die binnen die wet- en regelgeving bedacht is. Het is aan de lijnmanager om te beoordelen welke risico's er binnen de processen zijn en hoe deze risico's het beste kunnen worden beperkt. De lijnmanagers dienen er onder andere op toe te zien dat de controle op het verwerken van (persoons)gegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste (persoons)gegevens ingezien en verwerkt hebben. Ook dienen zij erop toe te zien dat de bedrijf continuïteit binnen hun proces is gegarandeerd.

5.1.7.1 Ketenverantwoordelijkheid

De verschillende informatiesystemen in onze organisatie zijn vaak onderling afhankelijk en ondersteunen samen een bepaald proces. Bovendien kunnen informatiesystemen van verschillende organisaties een keten vormen die verder reikt dan onze gemeentelijke organisatie. Om deze reden wijst de directie voor een keten altijd één lijnmanager aan als proceseigenaar. Deze proceseigenaar stelt het beveiligingsniveau voor de keten vast, rekening houdend met specifieke afspraken binnen deze keten.

De lijnmanagers zijn eigenaar van de ondersteunende applicaties binnen dit proces. Daar waar applicaties worden gebruikt in meerdere bedrijfsprocessen geldt dat het bedrijfsproces met het hoogst noodzakelijke beveiligingsniveau leidend is. Alle processen, systemen, (persoons)gegevens, applicaties dienen altijd minimaal 1 eigenaar te hebben; er moet dus altijd iemand verantwoordelijk zijn.

Processen, applicaties en systemen zonder eigenaar worden door de directie toegewezen aan een lijnmanager, zodat de verantwoordelijkheden altijd belegd zijn. Het Directieberaad zorgt ervoor dat centraal wordt vastgelegd welke lijnmanager als 'eigenaar' fungeert voor de gemeentelijke processen en applicaties en ketens en daarmee ook verantwoordelijk is voor de bijbehorende informatiebeveiliging.

5.1.8 Chief Information Security Officer (CISO)

De rol van de CISO is vooral adviserend. De CISO treedt op als strategisch adviseur voor het bestuur, directie en het management. De CISO adviseert over het strategisch informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging overeenkomstig de behoeften en de risicobereidheid van de gemeente.

De CISO is verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid. De CISO ondersteunt directie en bestuur vanuit een onafhankelijke positie en heeft de mogelijkheid om rechtstreeks gevraagd en ongevraagd aan de directie en/of portefeuillehouder te rapporteren over de stand van zaken van informatiebeveiliging. Het advies van de CISO is zwaarwegend bij het nemen van beslissingen. De CISO is in het kader van het verantwoordingstraject informatiebeveiliging daarnaast ook coördinator ENSIA. Vanuit de BIO is het aanstellen van een CISO een verplichte overheidsmaatregel.

5.1.9 ENSIA coördinator

De ENSIA-coördinator is verantwoordelijk voor het organiseren en coördineren van de jaarlijkse verantwoording voor informatiebeveiliging (ENSIA- verantwoording) richting de gemeenteraad en toezichthouders van het Rijk.

De CISO en ENSIA-coördinator zijn beide gericht op informatiebeveiliging en Gegevensbescherming, maar hebben verschillende verantwoordelijkheden en focuspunten. De CISO is een strategisch adviseur in het kader van informatiebeveiliging en de ENSIA-coördinator is gericht op het coördineren en uitvoeren van de verantwoording ENSIA.

5.1.10 Information Security Officer (ISO)

De ISO ondersteunt het lijnmanagement en de CISO bij informatiebeveiliging. De ISO ondersteunt bij de implementatie en uitvoering van informatiebeveiligingsbeleid en bij projecten, en ondersteunt bij het uitvoeren van risicoanalyses op securityvlak. De ISO valt hierarchisch onder de manager Informatievoorziening en legt hier verantwoording af. De ISO ontvangt ten aanzien van zijn taken richtinggevend advies van de CISO.

5.1.11 Beveiligingsbeheerder

De beveiligingsbeheerder is verantwoordelijk voor het beheer, de coördinatie en het advies ten aanzien van de informatiebeveiliging binnen een specifiek deelgebied.

De beveiligingsbeheerder is een kwaliteitsmedewerker en is decentraal gepositioneerd voor het borgen van specifiek voor die afdeling of proces geldende wetgeving. Voorbeelden hiervan zijn Basisregistratie Personen, Reisdocumenten (officieel beveiligingsfunctionaris Reisdocumenten) en Suwinet (officieel Security Officer Suwinet).

5.1.12 Medewerker Kwaliteit en Control
De medewerker Kwaliteit en Control voert verbijzonderde interne controles uit op de naleving van informatiebeveiligingsbeleid en overige wet- en regelgeving.

5.1.13 Procesondersteuner
De procesondersteuner is een medewerker binnen een afdeling (bijvoorbeeld een functioneel beheerder) en ondersteunt de (lijn)manager. De procesondersteuner voert informatiebeveiliging door in de processen conform wet- en regelgeving.

De procesondersteuner is direct betrokken bij de implementatie van het informatiebeveiligingsbeleid en kent de processen en relevante wetgeving. De procesondersteuner rapporteert periodiek over de informatieveiligheid aan de (lijn)manager en ENSIA coördinator. De procesondersteuner zorgt voor de inhoudelijke aanlevering nodig bij de ENSIA verantwoording.

5.2 Externe partijen

5.2.1 Externe Dienstverlener
Met alle leveranciers die in de vorm van (kantoor)automatisering, applicaties, IT-componenten en/of operationele technologie informatie van de Dommelvallei-organisaties verwerken of operationele processen aansturen, dienen afspraken gemaakt te worden op welke wijze zij de informatiebeveiliging borgen en leggen hier periodiek (volgens gemaakte afspraak) verantwoording over af aan de proceseigenaar. Bijvoorbeeld via een Third Party Memorandum of Third Party Mededeling. Dit is een verklaring die wordt afgegeven door een onafhankelijke auditpartij.

5.2.2 Rekenkamercommissie (alleen Gemeenten)
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 en rapporteert hierover aan de gemeenteraad.

5.2.3 Externe partij in een samenwerkingsverband
Een externe partij in samenwerkingsverband is verantwoordelijk om de verwerkte gegevens in de keten te beveiligen. Dit kan bijvoorbeeld een ketenpartner of een gemeenschappelijke regeling zijn. Publieke partijen zijn verplicht zich te houden aan de Baseline Informatiebeveiliging Overheid (BIO), terwijl private partijen niet direct gebonden zijn aan de BIO en zich daarom aan een schriftelijke dienstverlenings-, verwerkersovereenkomst moeten houden. Als een gemeente haar taken heeft belegd binnen een samenwerkingsverband (o.a. Gemeenschappelijke Regeling), blijft de gemeente eindverantwoordelijk voor de borging van de informatieveiligheid. Per samenwerkingsverband zal onderzocht moeten worden op welke wijze de verantwoordelijkheden zijn belegd.

5.2.4 Externe Auditor
Een externe auditor is een partij die in opdracht van de Dommelvallei-organisaties een onafhankelijk onderzoek uitvoert om de naleving van het informatiebeveiligingsbeleid en wet- en regelgeving te beoordelen.

5.2.5 Informatiebeveiligingsdienst voor Gemeenten (IBD)
De IBD[11] is een onderdeel van de Vereniging Nederlandse Gemeenten (VNG) en levert ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. De Dommelvallei-organisaties maken gebruik van deze ondersteuning. De IBD informeert ons via vastgestelde contactpersonen namelijk de algemeen contactpersoon informatiebeveiliging (ACIB)[12] en de vertrouwde contactpersoon informatiebeveiliging (VCIB)[13]. Hiervoor zijn onder andere aangewezen de CISO en collega's van systeembeheer.

11) De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD ondersteund specifiek gemeenten bij het werken aan weerbaarheid op het gebied van informatiebeveiliging. Hierin zit ook incidentbeheer en incidentpreventie.

12) Algemene waarschuwingen en informatie met een niet vertrouwelijk karakter

13) Informatie die vertrouwelijk is van karakter

6 Overlegstructuur met stakeholders

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

Overleg	Deelnemers	Frequentie	Toelichting
Bestuur Dienst Dommelvallei Strategisch niveau	3 burgemeesters en 3 wethouders, CISO, FG, manager IV	2x per jaar	- Adviseren ingeval van nieuwe wetgeving, ontwikkelingen en advies benodigde middelen. - Voorbespreken stukken aan college BW gemeente en raadsvoorstellen/RIB - Potentiële dreigingen die leiden tot bestuurlijke risico's - Vaststellen strategisch informatiebeveiligingsbeleid
Directieberaad Strategisch/ tactisch niveau	4 Directeuren CISO, FG	1 x vast moment i.v.m. bestuursrapportage en incidenteel op afroep[14]	- Voorbespreken stukken aan Bestuur Dienst Dommelvallei en Bestuur gemeenten - Vaststellen tactisch informatiebeveiligingsbeleid - Vasstellen plan van aanpak ENSIA - Sturen op strategisch/ tactisch informatiebeveiligingsrisico's
Periodiek overleg overleg Directeur Dienst Dommelvallei Strategisch/ tactisch niveau	FG, CISO en Directeur	Maandelijks	- Voorbereidingen input Directieberaad - Informeren stand van zaken, ontwikkelingen
OGON Tactisch - operationeel niveau	Vaste medewerkers OGON, CISO en ISO[15]	4 x per jaar	- Monitoren en sturing op informatiebeveiliging op hoofdlijnen - Sturen op tactische /operationele risico's - Afstemmen beleidskaders voorafgaand aan vaststelling Directieberaad. - Organiseren integrale aanpak procesmatig werken
Periodiek overleg informatiebeveiliging Tactisch- operationeel niveau	Manager IV, systeembeheerders en CISO, ISO	1 x per maand	- Tactisch beleid vertalen naar uitvoering - Bespreken stand van zaken, ontwikkelingen
Weekstart informatiebeveiliging en privacy Strategisch – Tactisch - Operationeel	CISO en FG	wekelijks	- Informeren en onderling afstemmen lopende onderwerpen - Afhankelijk van onderwerp en advies betreft dit strategisch- tactisch of operationeel
Privacy overleg Operationeel	FG en privacy officers CISO incidenteel op afroep	Maandelijks	- Bespreken stand van zaken en ontwikkelingen aanhakende thema's

14) Waarbij geldt dat stukken die in het college worden besproken via Directieberaad worden ingebracht.
15) Ook collega's van de thema's zoals privacy en archivering sluiten op deze overlegstructuur aan.

Kick-off ENSIA verantwoording Tactisch - operationeel	Directeur Dienst Dommelvallei, proceseigenaren, managers bedrijfsvoering, concernmanager, proces-ondersteuners, beveiligings-beheerders, CISO	Jaarlijks	- Informeren over plan van aanpak ENSIA proces, scope en verwachtingen-management
Informatie-beveiliging crisisoverleg Strategisch - Tactisch	Afhankelijk van incident: Directeur, Burgemeester CISO, privacy officer, verantwoordelijke voor het proces waar de crisis betrekking op heeft, Communicatie en/of FG	Zodra zich een incident voordoet	- Ondervangen en grip krijgen op crisis - Input voor analyse en rapportage van incident - Afhankelijk van soort crisis strategisch/ tactisch.

7 Rapportagemomenten informatiebeveiliging

Periodieke rapportages vloeien voort uit bovengenoemde contactmomenten met stakeholders. Rapportages worden opgesteld van incidenten, het verantwoordingstraject ENSIA en periodieke inzicht in de stand van zaken van informatiebeveiliging (P&C-cyclus). Aangezien het College en de Raad met name een rol spelen in het verantwoordingstraject, wordt deze verantwoording in onderstaande paragraaf toegelicht.

7.1 Jaarlijkse verantwoording ENSIA

Ter afsluiting van de jaarlijkse verantwoording ENSIA rapporteren de lijnmanagers over de risico's binnen hun bedrijfsprocessen en over de stand van zaken van de implementatie van informatiebeveiliging van het afgelopen jaar. Zij rapporteren aan de directie. Dit doen zij via de jaarlijkse ENSIA verantwoording. De ENSIA coördinator coördineert dit proces.

In het plan van aanpak ENSIA dat jaarlijks wordt opgesteld, is een detailplanning opgenomen van deze jaarlijkse verantwoording, waarop tussentijds wordt gemonitord. De ENSIA coördinator stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de lijnmanagers/proceseigenaren een bestuurlijke rapportage op.

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.