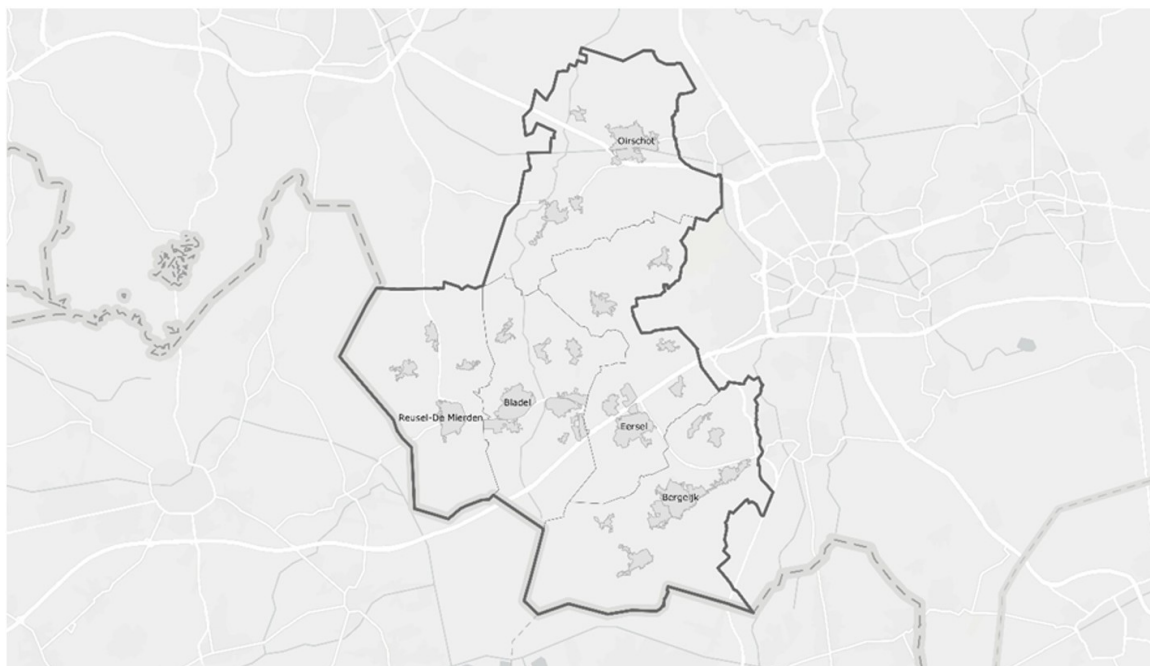


Informatiebeveiligingsbeleid 2025

Kempengemeenten (Bergeijk, Bladel, Eersel, Oirschot, Reusel-De Mierden)
Gemeenschappelijke Regeling Samenwerking Kempengemeenten
Gemeenschappelijke Regeling Participatiebedrijf KempenPlus



Managementsamenvatting

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan vertrouwelijke informatie over zowel inwoners als bedrijven. Daarnaast zijn gemeenten verantwoordelijk voor een betrouwbare en continue dienstverlening. De Kempengemeenten (Bladel, Bergeijk, Eersel, Oirschot en Reusel-De Mierden), de Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK) en de Gemeenschappelijke Regeling Participatiebedrijf KempenPlus (KempenPlus) (hierna samen te noemen Kempenorganisaties) hebben zich het doel gesteld om informatiebeveiliging gezamenlijk op te pakken om een eenduidige werkwijze voor informatiebeveiliging te bevorderen en het beheer van informatiebeveiliging te vereenvoudigen en te versterken.

Dit informatiebeveiligingsbeleid biedt een kader voor de Kempenorganisaties om informatie op een passende wijze te beveiligen. Dit informatiebeveiligingsbeleid vervangt het 'Informatieveiligheidsbeleid Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempengemeenten 2020'.

Het kader, en daarmee ook dit beleid, is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast verwijst het beleid naar aanverwante wet- en regelgeving. De reikwijdte van dit beleid omvat daarom de bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de Kempenorganisaties in de meest brede zin van het woord.

Belangrijke uitgangspunten hierbij zijn:

- Informatiebeveiliging is en blijft een verantwoordelijkheid van de hele organisatie. Voor de Kempenorganisaties ligt de bestuurlijke verantwoordelijkheid voor informatiebeveiliging bij de colleges van Burgemeester en Wethouders. Bij de gemeenschappelijke regelingen is het (Dagelijks-) Bestuur eindverantwoordelijk voor de informatiebeveiliging.
- Informatiebeveiliging is risicomanagement: een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen.

Daarnaast beschrijft het beleid de rollen, taken en verantwoordelijkheden in de Kempenorganisaties ten aanzien van informatiebeveiliging en hoe ervoor gezorgd kan worden dat informatiebeveiliging geborgd blijft binnen de Kempenorganisaties.

In het beleid is een groeimodel aangegeven waar de Kempenorganisaties naar toe willen groeien om de beveiliging op een hoger niveau te brengen om aan gestelde normen te voldoen. Via een informatiebeveiligingsplan, dat jaarlijks bijgesteld wordt, werken de Kempenorganisaties aan het realiseren van de in het groeimodel genoemde doelen. Het informatiebeveiligingsbeleid dient minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld en zo nodig te worden bijgesteld.

1. Inleiding

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor Kempenorganisaties om hun processen uit te voeren. Kempenorganisaties beschikken over een schat aan vertrouwelijke (persoons-)gegevens van inwoners en bedrijven. Daarnaast zijn Kempenorganisaties verantwoordelijk voor een betrouwbare en continue dienstverlening. Onze inwoners vertrouwen erop dat de Kempenorganisaties haar vertrouwelijke gegevens afdoende beveiligen. Het is daarom belangrijk dat informatie op passende wijze beveiligd wordt.

1.1 Doelstelling

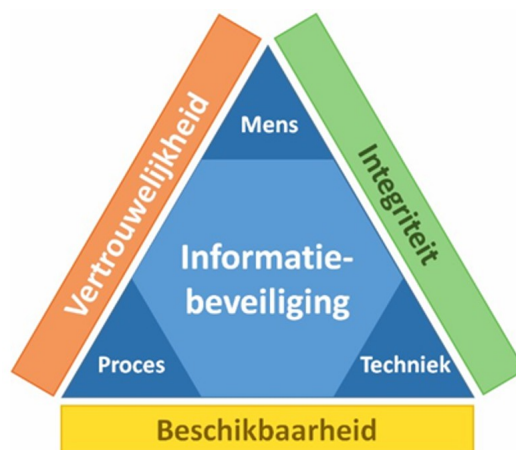
Het doel van dit beleid is het vastleggen van algemene beleidsuitgangspunten over informatiebeveiliging voor de Kempenorganisaties. Het beleid is gebaseerd op de implementatie van de Baseline Informatiebeveiliging Overheid 2 (BIO2) en voldoen aan NIS2 met daarbij het mitigeren van de risico's welke door de eindverantwoordelijke worden bepaald. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. De uitwerking van dit beleid naar concrete maatregelen wordt vastgelegd in een jaarlijks bij te stellen informatiebeveiligingsplan.

Dit beleid vervangt het huidige informatiebeveiligingsbeleid 'Informatieveiligheidsbeleid Kempengemeenten, Gemeenschappelijke Regeling Samenwerking Kempengemeenten en Gemeenschappelijke Regeling Participatiebedrijf KempenPlus 2020'.

1.2 Definitie informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket van maatregelen, procedures en processen, die er gezamenlijk voor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie op het juiste niveau wordt gewaarborgd. Voor het ene proces is vertrouwelijkheid van informatie belangrijker, voor het andere beschikbaarheid of integriteit. Hieronder is weergegeven wat de Kempenorganisaties verstaan onder deze begrippen.

Beschikbaarheid/ continuïteit	Het zorg dragen voor het beschikbaar zijn van informatie en informatiesystemen op de juiste tijd en plaats voor de gebruikers.
Integriteit/ betrouwbaarheid	Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
Vertrouwelijkheid/ exclusiviteit	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.



1.3 Leeswijzer

In dit beleid is beschreven wat de Kempenorganisaties willen bereiken met informatiebeveiliging en op basis van welke kaders en uitgangspunten voor informatiebeveiliging dit georganiseerd wordt. Vervolgens is beschreven hoe de rollen en verantwoordelijkheden zijn belegd om informatiebeveiliging goed te organiseren. Tenslotte is aan de hand van de BIO weergegeven welke informatiebeveiligingsdoelen bereikt moeten worden om te groeien naar een accurate beveiliging van de gemeentelijke informatie en informatiesystemen.

Het informatiebeveiligingsbeleid moet daarnaast gezien worden als een overkoepelend beleidsstuk, waarbij in onderliggende plannen, documentatie, procedures en instructies verdere detaillering en afspraken worden vastgelegd.

2. Scope van het informatiebeveiligingsbeleid

Informatiebeveiliging is meer dan IT, computers en automatisering. Het gaat om alle uitingvormen van informatie, alle mogelijke informatiedragers en alle informatie verwerkende systemen, maar vooral ook menselijk handelen en processen.

De scope van dit beleid omvat alle gemeentelijke informatieprocessen, informatie en gegevens van zowel de Kempenorganisaties als externe partijen en de onderliggende informatiesystemen. Het beleid heeft betrekking op het gebruik en de verwerking, uitwisseling en opslag van zowel digitale als analoge informatie, ongeacht de locatie, het tijdstip en gebruikte apparatuur.

Dit informatiebeveiligingsbeleid is een algemene basis voor informatiebeveiliging. Het beleid dekt tevens aanvullende beveiligingseisen uit wetgeving af, zoals voor de BRP, Suwi, de BIO2, de DigiD-norm B.01 en de aanstaande Cyberbeveiligingswet (Cbw). Voor bepaalde kerntaken gelden op grond van deze eisen, naast wet- en regelgeving, nog enkele specifieke (aanvullende) beveiligingseisen. Deze worden in aanvullende documenten geformuleerd. Bewust wordt in dit strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar dit overkoepelende beleid gelegd.

De BIO2 wordt het nieuwe (verplichte) normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teammanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001/27002 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is.

Voor de nieuwe wet Cbw is het onder andere essentieel om 'opzet, bestaan en werking' goed aantoonbaar te maken, omdat wij aan dit strengere regime moeten gaan voldoen. Omdat deze nieuwe wet de verantwoording expliciet legt bij bestuur, directie en management is het van belang dat hier eisen aan worden gesteld en dat er controle op wordt uitgevoerd.

3. Kaders & uitgangspunten

3.1 Kaders

De basis voor dit informatiebeveiligingsbeleid is de NEN-ISO/IEC 27002:20017 en het daarvan afgeleide normenkader informatiebeveiliging voor de gehele overheid, de BIO. Aanvullend hierop worden de 10 bestuurlijke principes voor informatiebeveiliging als kader gevolgd. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

Aanvullend worden op basis van algemene wet- en regelgeving (bijvoorbeeld; niet uitputtend: AVG, BRP, SUWI) en aanvullende beveiligingsnormen, maatregelen getroffen op het gebied van informatiebeveiliging.

Op basis van bovenstaande kaders zijn de volgende strategische doelen geformuleerd:

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

3.2 Uitgangspunten

De kaders en strategische doelen zijn vertaald naar de volgende uitgangspunten:

- Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de Kempenorganisaties. Bij de gemeenten is het college van Burgemeester en Wethouders eindverantwoordelijk voor de informatiebeveiliging. Bij de Gemeenschappelijke Regelingen is het (Dagelijks-) Bestuur eindverantwoordelijk.
- De uitvoering van informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Zij draagt verantwoordelijkheid voor de uitvoering, ondersteuning en bewaking van dit informatiebeveiligingsbeleid en draagt dit uit naar de organisatie. Proceseigenaren, systeemeigenaren en gegevenseigenaren hebben ieder hun eigen, maar ook gezamenlijke verantwoordelijkheid ten aanzien van informatiebeveiliging en het uitdragen hiervan. De verantwoordelijkheden voor informatiebeveiliging worden expliciet gedefinieerd.
- De organisatiebrede CISO- binnen de Kempenorganisaties aangeduid als CISO of informatiebeveiligingsfunctionaris – ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hier rechtstreeks over aan de directie.
- Het primaire uitgangspunt van informatiebeveiliging is risicomanagement. Om de informatiebeveiliging af te stemmen op interne en externe ontwikkelingen worden minimaal tweejaarlijks risicoanalyses uitgevoerd. Of eerder indien wijzigingen in de omgeving, technische wijzigingen of dreigingsveranderingen hier aanleiding voor geven.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check, act;' vormen samen het managementsysteem van informatiebeveiliging. De Kempenorganisaties legt jaarlijks verantwoording af over haar informatiebeveiliging via de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit).
- Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie en de ketenpartners. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament voor een betrouwbare informatievoorziening. Het plan bevat een concrete vertaling van het informatiebeveiligingsbeleid naar te nemen maatregelen om de informatiebeveiligingsdoelen te waarborgen. Het informatiebeveiligingsplan wordt jaarlijks geactualiseerd vastgesteld.
- De Kempenorganisaties stellen de benodigde mensen en middelen beschikbaar om haar eigen domeinen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden ten aanzien van het informatiebeveiligingsbeleid worden vastgesteld.
- Iedere medewerker, zowel vast of tijdelijk, intern of extern, is verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en hiervan bij (vermeende) inbreuk melding te maken.

4. Visie informatiebeveiliging

4.1 Het belang van informatiebeveiliging

De Kempenorganisaties ontwikkelen gezamenlijk een toekomstgericht informatielandschap. Hierin worden de gemeentelijke dienstverlening en bedrijfsprocessen steeds meer digitaal vormgegeven. Daarbij zijn klant- en servicegerichtheid, efficiëntie, gebruiksgemak en snelheid van grote waarde voor zowel de Kempenorganisaties als haar inwoners. Een belangrijke ontwikkeling is dat de Kempenorganisaties voor de uitvoering van taken over het brede spectrum van beleidsterreinen steeds meer gebruik maken van diverse mogelijkheden van informatie-uitwisseling, zowel onderling als met diverse ketenpartners. Het netwerk van informatie-uitwisseling ontwikkelt zich nog steeds. Met het stelsel van basisregistraties krijgen de Kempenorganisaties ook steeds breder toegang tot landelijke gegevensvoorzieningen. Informatie is een cruciaal bedrijfsmiddel voor de Kempenorganisaties.

Vanwege het cruciale belang van informatie voor de Kempenorganisaties, is het noodzakelijk dat de informatiebeveiliging professioneel georganiseerd is en gegevens van inwoners beschermd worden. Gegevens dienen beschikbaar, betrouwbaar en alleen door bevoegden inzichtelijk zijn. Verlies of manipulatie van informatie, uitval van systemen of het inzien van informatie door onbevoegden kan ernstige gevolgen hebben voor de bedrijfsvoering. Beveiligingsincidenten kunnen negatieve gevolgen hebben voor inwoners, bedrijven en organisaties, wat mogelijk leidt tot imagoschade en politieke consequenties voor de Kempenorganisaties.

4.2 Visie

Een betrouwbare informatievoorziening is noodzakelijk voor het functioneren van de gemeentelijke organisatie. De Kempenorganisaties beveiligen haar systemen en processen om uitval van vitale processen en dienstverlening te voorkomen. Daarnaast is het de plicht van de Kempenorganisaties om de privacybescherming van haar inwoners, bedrijven en organisaties te waarborgen. De beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van gegevens, ongeacht hun verschijningsvorm, dienen geborgd te zijn.

Risicobeheersing is het uitgangspunt bij informatiebeveiliging. Schade wordt geminimaliseerd door het zo veel mogelijk voorkomen van beveiligingsincidenten. De Kempenorganisaties hanteren daarbij een integrale aanpak. Op basis van risicomanagement worden zowel technische als organisatorische maatregelen genomen om schade te voorkomen of te beperken. Dat gaat verder dan het regelen van beveiliging met IT. Informatiebeveiliging is een organisatie breed onderwerp dat de inrichting van processen en procedures door de hele organisatie raakt. Alle medewerkers zijn verantwoordelijk voor de waarborging van de informatiebeveiliging binnen hun functie. Verantwoord en bewust gedrag van medewerkers is essentieel voor informatiebeveiliging.

Adequate informatiebeveiliging is van essentieel belang voor de bedrijfsvoering en dienstverlening van de Kempenorganisaties. De Kempenorganisaties streven de volgende doelen na om een adequaat niveau van beveiliging conform de Baseline Informatiebeveiliging Overheid (BIO) en aanverwante wet- en regelgeving te bereiken:

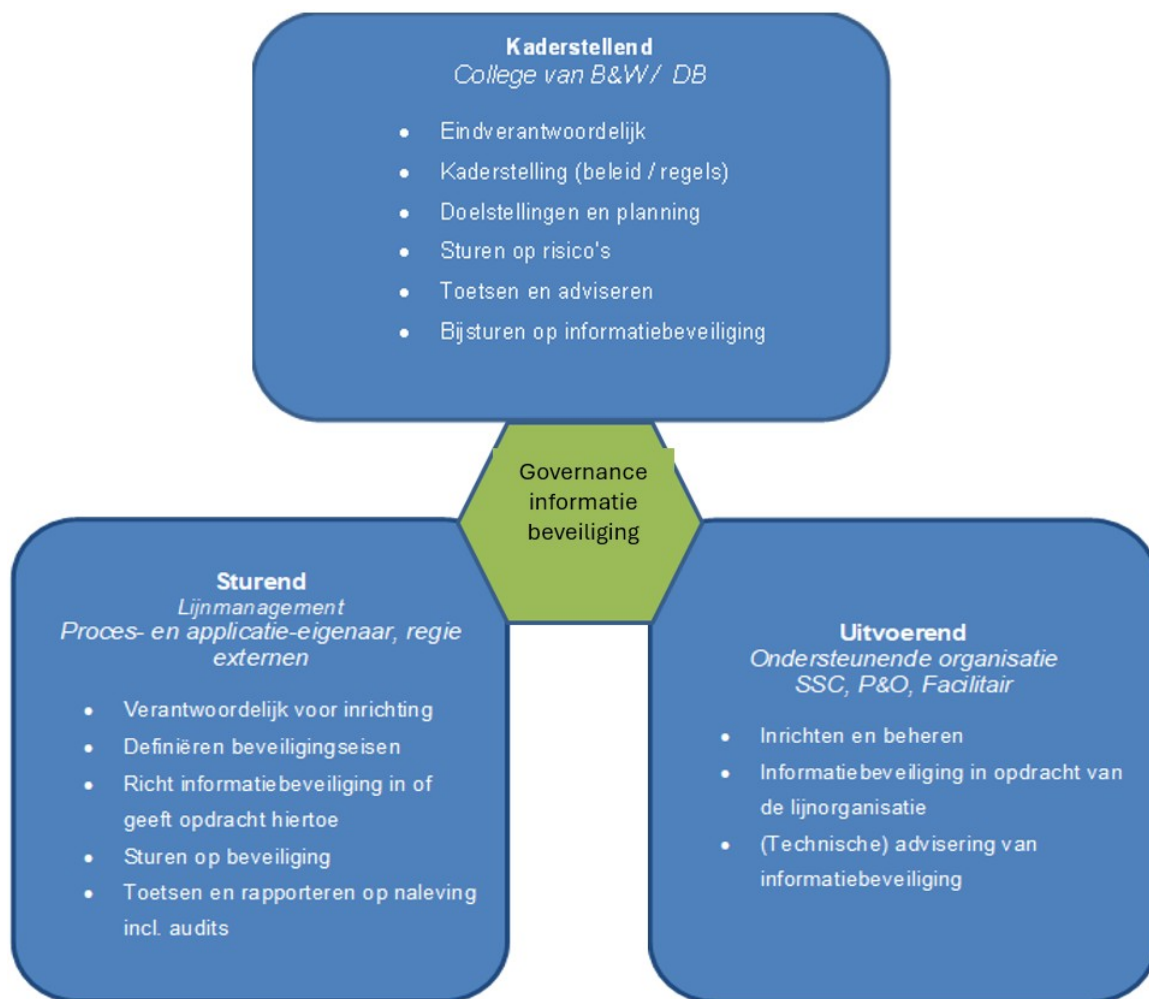
1. De Kempenorganisaties borgen de beveiligingseisen (controls) volgens de BIO door implementatie van aan de control gerelateerde informatiebeveiligingsmaatregelen.
2. De Kempenorganisaties zijn 'in control' over de geïmplementeerde informatiebeveiligingsmaatregelen, middels verankering in een PDCA-cyclus.
3. De Kempenorganisaties verankeren het onderwerp informatiebeveiliging in alle organisatieonderdelen, middels het actief aanwijzen van verantwoordelijkheden, rollen en taken voor informatiebeveiliging.
4. De Kempenorganisaties zorgen voor informatiebeveiligingsbewustzijn onder alle medewerkers (zowel intern als extern) en bestuurslagen.

5 Organisatie van Informatiebeveiliging

Dit hoofdstuk gaat in op de rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging. Daarnaast wordt uiteengezet hoe informatiebeveiliging wordt geborgd.

5.1 Rollen en verantwoordelijkheden

In dit onderdeel zijn de belangrijkste rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging beschreven. De precieze invulling van de rollen en verantwoordelijkheden dient te zijn beschreven in (onderliggende) beleidstukken, kaderstellingen, procedures en werkinstructies. De aansturing ten aanzien van informatiebeveiliging moet vooral komen vanuit organisatieonderdelen die verantwoordelijk zijn voor de bedrijfsprocessen en hun behoefte aan informatiebeveiliging. Er moet dus duidelijk onderscheid zijn tussen regie en uitvoering. Dit houdt mede in dat de lijnorganisatie de rol van opdrachtgever op zich neemt en ondersteunende organisatieonderdelen de uitvoerende rol op zich nemen. Het college van B&W en het DB bevinden zich in de sturende rol. Zij zetten de kaders uit en bepalen de doelen die behaald moeten worden.



5.1.1 Kaderstellend

Bij de implementatie van het informatiebeveiligingsbeleid hebben de besturen van de Kempenorganisaties belangrijke verantwoordelijkheden om ervoor te zorgen dat de organisaties voldoen aan het beleid. Enkele van deze verantwoordelijkheden zijn:

1. **Leiderschap en betrokkenheid:** Het bestuur moet leiderschap tonen en betrokken zijn bij het ontwikkelen en implementeren van het beleid;
2. **Risicobeheer:** Het bestuur is verantwoordelijk voor het waarborgen van een effectief risicobeheerproces, inclusief informatiebeveiliging;
3. **Toewijzing van middelen:** Het bestuur moet voldoende financiële, personele en technische middelen toewijzen om het beleid voldoende te kunnen implementeren;
4. **Naleving van wet- en regelgeving:** Het bestuur moet toezicht houden op de naleving van wet- en regelgeving met betrekking tot informatiebeveiliging, zoals de BIO2, NIS2-richtlijn en andere relevante wetgeving (bijvoorbeeld AVG);
5. **Cultuur van informatiebeveiliging:** Het bestuur moet een cultuur van informatiebeveiliging bevorderen binnen de organisatie en zorgen voor bewustwording en training van medewerkers op het gebied van cyberbeveiliging en de naleving van het informatiebeveiligingsbeleid. Zo worden er voorlichtingsmeetings gegeven aan nieuwe medewerkers en worden medewerkers proactief op de hoogte gehouden van de nieuwste ontwikkelingen op het gebied van informatiebeveiliging. Daarnaast worden hun vragen m.b.t. informatiebeveiliging beantwoord;
6. **Regelmatige (jaarlijkse) evaluatie en verbetering:** Het bestuur moet toezicht houden op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen en zorgen voor continue verbetering van de informatiebeveiliging in overeenstemming met de vereisten van het informatiebeveiligingsbeleid.

5.1.2 Sturend

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. De directie zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college of (Dagelijks) bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college of het (Dagelijks) bestuur zich ook verantwoorden naar de raad of (Algemeen) bestuur.

De directie stelt het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO's van de Kempenorganisaties. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de Kempenorganisaties gezien als een integraal onderdeel van risicomanagement.

5.1.3 Uitvoerend

Informatiebeveiliging valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de teammanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures;
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures;
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen;
- Voorbereiding en coördinatie van het overleg ligt bij de CISO.

In bijlage 2 zijn de verschillende rollen en verantwoordelijkheden voor informatiebeveiliging verder uitgewerkt.

5.2 Borging en verantwoording informatiebeveiliging

Informatiebeveiliging is een continu verbeterproces. Om te waarborgen dat informatiebeveiliging niet slechts een eenmalige actie is, dient informatiebeveiliging te zijn geborgd in de organisatie. De besturen van de Kempenorganisaties zijn verantwoordelijk voor de borging van dit informatiebeveiligingsbeleid en de controle hierop.

De Kempenorganisaties verantwoorden zich jaarlijks over hun informatiebeveiliging middels de ENSIA-systematiek. De verantwoording over de informatiebeveiliging komt tot uitdrukking in het jaarverslag van de Kempenorganisaties en de verschillende beveiligingsrapportages die volgen uit ENSIA. Op basis van de rapportages worden verbetermaatregelen geformuleerd en opgenomen in het informatiebeveiligingsplan.

ENSIA is een landelijk gestandaardiseerd verantwoordingsinstrument dat gemeenten ondersteunt bij het afleggen van verantwoording over de informatiebeveiliging. ENSIA staat voor Eenduidige Normatiek Single Information Audit. Het stelt gemeenten in staat om op een gestructureerde en uniforme manier aan te tonen dat zij voldoen aan de normen van de BIO. ENSIA toetst door middel van zelfevaluaties en een externe audit, voor de DigiD- en Suwinet-aansluitingen, de kwaliteit van de informatiebeveiliging en basisregistraties.

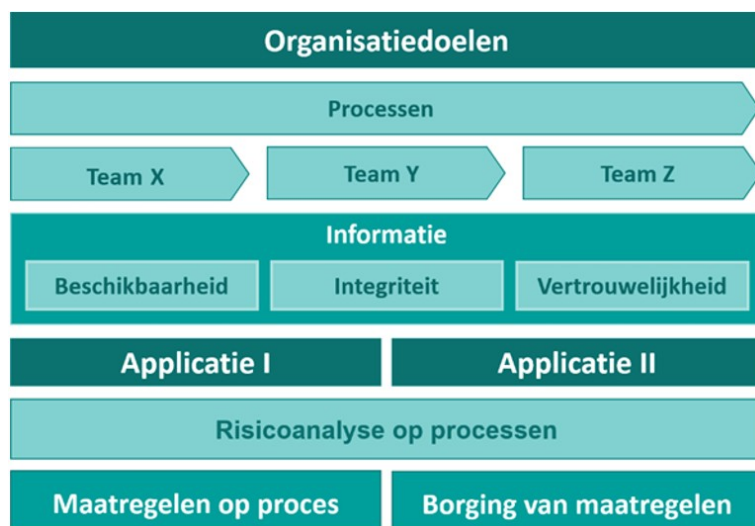
Binnen de organisatie is er één ENSIA-coördinator aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van de vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke ambtenaar. De ambtenaar levert alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijst.

ENSIA draagt bij aan de continue verbetering en borging van informatiebeveiliging binnen de gemeentelijke organisatie. De verantwoording over informatieveiligheid sluit aan op de planning en control-cyclus van de gemeente. Middels de ENSIA-verantwoording wordt er interne verantwoording over de informatiebeveiliging afgelegd aan de gemeenteraad en externe verantwoording aan toezichthouders van het Rijk. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente informatiebeveiliging serieus neemt en het onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Daarnaast wordt het een verplichting om een Information Security Management System (ISMS) aan te leggen. In een ISMS worden alle werkzaamheden, besluiten, risico's en maatregelen beschreven. Het ISMS is dus niet alleen een middel om de stand van zaken in bij te houden, maar ook het proces dat jaarlijks wordt doorlopen om de informatieveiligheid binnen de Kempenorganisaties te verbeteren. Het ISMS wordt door iedereen gevoed die werkt aan de informatiebeveiliging en voor de CISO en management is het ook een middel om sturing te geven aan het continue verbeteren van de informatiebeveiliging.

6. Risicomanagement

Informatiebeveiliging wordt vaak gezien als iets wat er extra bij komt. Informatiebeveiliging ligt echter ten grondslag aan het organisatiedoel dat bereikt dient te worden. Om een doel te bereiken, dienen processen uitgevoerd te worden waarvoor informatie (vaak in meerdere softwareapplicaties) wordt verwerkt. Een goede afweging van de risico's helpt om de juiste maatregelen te treffen om de gegevens in deze processen te beschermen. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Tenslotte moeten deze maatregelen in de organisatie geborgd worden, zodat de Kempenorganisaties aantoonbaar grip houden op de veiligheid.



100% beveiliging bestaat niet en dient ook niet nagestreefd te worden. De kosten en inspanningen van informatiebeveiliging moeten in verhouding zijn tot de risico's. De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in de Kempenorganisaties is daarom ook op basis van risicoafweging. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's. Daarnaast dienen de Kempenorganisaties goed te zijn voorbereid op incidenten en crises. Het informatiebeveiligingsrisico is de som van de kans op beveiligingsincidenten en de impact daarvan op het werkproces: $\text{risico} = \text{kans} \times \text{impact}$.

Risicomanagement is een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen. De proceseigenaar dient periodiek de risico's te beoordelen. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligings-eisen van de informatie. De proceseigenaar neemt indien nodig maatregelen om de risico's te beperken. De CISO kan hierbij ondersteunen in zowel techniek van risicoanalyse als bij de inhoudelijke analyse zelf. Hierbij kunnen ook systeemeigenaren en procesdeskundigen ondersteunen.

De benadering op basis van risicoafweging betekent ook dat gefundeerd afgeweken kan worden van de BIO indien de Kempenorganisaties hier een geaccepteerd risico lopen. Tegelijkertijd houdt dit in dat

mogelijk meer maatregelen getroffen moeten worden ten opzichte van de baseline indien de Kempenorganisaties een hoog risico lopen. Op deze wijze worden tijd, geld en middelen passend besteed met als gevolg een stelsel van beveiligingsmaatregelen dat bij de Kempenorganisaties past.

7. Groei naar Informatiebeveiliging

In de voorgaande hoofdstukken van het beleid zijn de kaders, uitgangspunten en organisatie van de informatiebeveiliging beschreven. In dit hoofdstuk is aangegeven welke stappen de Kempenorganisaties tenminste dienen te nemen om te groeien naar een voldoende niveau van informatiebeveiliging.

7.1 Volwassenheidsniveaus

Per informatiebeveiligingsgebied is een ontwikkeldoel weergegeven hoe de organisaties gaan voldoen aan de BIO en hoe de organisaties op een hoger volwassenheidsniveau komen. In onderstaande tabel staan de volwassenheidsniveaus weergegeven. De Kempenorganisaties hebben zich ten doel gesteld om voor alle structurele processen in de organisatie tenminste op volwassenheidsniveau 3 te opereren.

Niveau	Naam	Omschrijving	Criteria
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte beheersmaatregelen geïmplementeerd. • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2	Herhaalbaar maar intuïtief	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar informele wijze uitgevoerd.	• Maatregelen zijn geïmplementeerd • Uitvoering is consistent en standaard • Informeel en grotendeels gedocumenteerd • Inconsistente wijze van meten en controleren
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar.	• Maatregelen zijn gedefinieerd op basis van risicoafweging • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken zijn eenduidig toegewezen • Controle en monitoring ontstaat • Opzet, bestaan en effectieve werking zijn aantoonbaar
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd en kwalitatief gecontroleerd.	• Periodieke (control) evaluatie en opvolging vindt plaats • Rapportage richting management vindt plaats
5	Continu verbeteren	Het systeem van beheersmaatregelen is verankerd in de organisatie en draagt zorg voor een continue en effectieve controle en risicobeheersing.	• Self-assessments en gap-analyses worden uitgevoerd • Real time monitoring • Inzet slimme automatisering

7.2 Groeimodel

Tot de inwerkingtreding van de Cbw, medio 2026, blijft de BIO1.04 van kracht. Het is echter wel de bedoeling dat BIO2 tot de inwerkingtreding Cbw als richtinggevend kader wordt toegepast. Hieronder de doelen van de Kempenorganisaties in relatie tot BIO1.04. De doelen zullen ook in BIO2 gelijk zijn, echter kan het mogelijk zijn dat deze in een ander hoofdstuk van BIO2 zijn opgenomen. Op dit moment is er nog geen was-woordt document beschikbaar.

7.2.1 Beveiligingsbeleid – BIO Hoofdstuk 5

Doel:

Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatiebeveiliging.

Onderliggende beleidstukken, kaderstellingen, procedures en werkinstructies zijn opgesteld zodat processen op gestructureerde en geformaliseerde wijze worden uitgevoerd en informatiebeveiliging in overeenstemming met het beleid is. De uitvoering is aantoonbaar.

7.2.2 Organiseren van informatiebeveiliging – BIO Hoofdstuk 6

Doel:

Het benoemen van het eigenaarschap van bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.

Informatiebeveiliging borgen in de organisatie door duidelijk gedefinieerd te hebben wie waarvoor verantwoordelijk is. Er wordt een proces opgezet dat zorgt voor continue borging en verbetering. Het lijnmanagement stuurt op eigenaarschap. Bij veranderingen en vernieuwingen (onder andere van applicaties) zorgt de eigenaar voor een gedegen risicoanalyse waarbij informatiebeveiliging standaard wordt beoordeeld.

7.2.3 Veilig personeel – BIO Hoofdstuk 7

Doel:

Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

(Externe) medewerkers zijn afdoende getraind en beschikken over de kennis van informatiebeveiliging die voor hun functie benodigd is. Hierbij is speciaal aandacht voor teamleiders/coaches, projectmanagers, proceseigenaren, systeemeigenaren, functioneel beheerders en functies die met gevoelige informatie of (bijzondere) persoonsgegevens werken.

Er is een beheerst instroom-doorstroom-uitstroom-proces dat waarborgt dat de juiste autorisaties en middelen tijdig en uitsluitend voor de juiste functies beschikbaar zijn. Dit proces is goed afgestemd op het autorisatieproces en is strak ingericht zodat het tijdig op veranderingen in de organisatie kan inspelen.

7.2.4 Beheer van bedrijfsmiddelen – BIO Hoofdstuk 8

Doel:

Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, informatie-systemen en bedrijfsmiddelen.

Elk bedrijfsmiddel dat een belang heeft voor de organisatie is verbonden aan een verantwoordelijke proces-, systeem-, of data-eigenaar. De verantwoordelijke kent op basis van de mate van beschikbaarheid, integriteit en vertrouwelijkheid de classificatie toe aan het bedrijfsmiddel. Dit bedrijfsmiddel is beschermd in overeenstemming met de hieraan toegekende classificatie. De Kempenorganisaties handhaven de bescherming van bedrijfsmiddelen zodat de informatie op een passend niveau beschermd blijft.

7.2.5 Toegangsbeveiliging – BIO Hoofdstuk 9

Doel:

Het beheersen van de toegang tot informatie en (informatie)systemen.

Er is een autorisatieproces dat waarborgt dat gebruikers toegang hebben tot de juiste systemen en applicaties en dat zij binnen applicaties over de juiste rechten beschikken. Op basis van risicoanalyse en afstemming op taken binnen verschillende rollen worden autorisaties bepaald.

Voor alle externe verbindingen waarmee toegang verkregen wordt tot gemeentelijke bedrijfsvertrouwelijke informatie dienen voldoende maatregelen te zijn getroffen om ongeautoriseerde toegang te voorkomen.

7.2.6 Cryptografie – BIO Hoofdstuk 10

Doel:

Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en integriteit van informatie te beschermen.

De Kempenorganisaties borgen de onweerlegbaarheid van verzending, ontvangst berichtenuitwisseling en het vertrouwd opslaan van bestanden. Hiervoor treffen de Kempenorganisaties correcte en doeltreffende cryptografische maatregelen. Hiermee zal de integriteit en vertrouwelijkheid van informatie worden beschermd tegen diefstal en misbruik.

7.2.7 Fysieke beveiliging en beveiliging van de omgeving – BIO Hoofdstuk 11

Doel:

De fysieke bescherming van gebouwen, terreinen, informatie en (informatie)systemen tegen onbevoegde fysieke toegang, schade of verstoring van continuïteit.

De middelen en gegevens, maar ook personen die benodigd zijn om de gemeentelijke processen uit te voeren zijn afdoende fysiek beschermd tegen uitval en tegen onbevoegd gebruik of inzage. Het geheel aan maatregelen kan per omgeving / gebouw verschillen, maar het beveiligingsniveau dient in overeenstemming te zijn met de dataclassificatie van de gegevens.

7.2.8 Beveiliging van bedrijfsvoering – BIO Hoofdstuk 12

Doel:

Correcte en veilige bediening van informatieverwerkende faciliteiten en nemen van maatregelen tegen het verlies van gegevens.

Het beheer van communicatie- en bedieningsprocessen omvat onder meer de processen rondom IT (waaronder wijzigingsbeheer, regie en controle ten aanzien van derde partijen, antivirus, back-up, netwerkbeveiliging, fysieke / digitale informatie-uitwisseling en logging). Bij al deze processen is het van belang dat de Kempenorganisaties minimaal op volwassenheidsniveau 3 opereren. Daarbij zijn maatregelen gedefinieerd, procedures gedocumenteerd en geformaliseerd en verantwoordelijkheden zijn eenduidig toegewezen. Hierbij dienen de maatregelen ook aantoonbaar en controleerbaar te zijn ingericht. Hierdoor kunnen onveilige situaties worden gedetecteerd en is structurele verbetering mogelijk.

7.2.9 Communicatiebeveiliging – BIO Hoofdstuk 13

Doel:

Het garanderen van correcte en veilige bediening en beheer van de IT-voorzieningen.

Het netwerk wordt op een juiste wijze beveiligd om risico's, zoals verminking, vernietiging, onderbreking, verwijdering of publicaties van informatie, te beheersen.

7.2.10 Acquisitie, ontwikkeling en onderhoud van informatiesystemen – BIO Hoofdstuk 14

Doel:

Het waarborgen dat beveiliging wordt ingebouwd in (informatie)systemen en dat beveiligingseisen worden meegenomen in het proces van systeemontwikkeling en -onderhoud.

Er is een beheerst en gedocumenteerd wijzigingsbeheerproces dat waarborgt dat wijzigingen in software en hardware afdoende worden beoordeeld op hun risico's. Er wordt getest zodat alleen goedgekeurde wijzigingen kunnen worden doorgevoerd. Hierdoor wordt de kans op incidenten en verstoringen beperkt. Naast software en hardware onder beheer van het SSC, geldt het wijzigingsbeheerproces ook voor applicaties onder beheer of regie van de lijnorganisatie. Dit proces is strak ingericht zodat het tijdig op veranderingen in de organisatie kan inspelen.

De Kempenorganisaties hebben een beheerst en gedocumenteerd proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat tenminste het tijdig verkrijgen van informatie over mogelijke kwetsbaarheden, risicoanalyse van kwetsbaarheden, het beheerst installeren van patches, en periodieke penetratietesten. Naast software en hardware onder beheer van het SSC, geldt het beheer van technische kwetsbaarheden ook voor applicaties onder beheer of regie van de lijnorganisatie.

Gegevensuitwisseling dient op een passende wijze te zijn beveiligd tegen inbreuken op integriteit en vertrouwelijkheid. Dit geldt voor de uitwisseling:

- binnen de grenzen van de gemeentelijke organisatie;
- tussen de Kempenorganisaties en andere organisaties of inwoners;
- (cloud-)applicaties van de Kempenorganisaties die extern van de gemeentelijke IT-infrastructuur opereren.

Op deze wijze wordt geborgd dat de Kempenorganisaties gezien worden als een betrouwbare partner betreffende de vertrouwelijkheid en integriteit van gegevens.

7.2.11 Leveranciersrelaties – BIO Hoofdstuk 15

Doel:

De bescherming van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

Binnen de Kempenorganisaties is contractmanagement dermate ingericht dat afspraken met de leveranciers duidelijk, transparant en controleerbaar zijn en dat hier actief op wordt gestuurd. Met de leverancier dienen informatiebeveiligingseisen te worden overeengekomen en gedocumenteerd.

7.2.12 Beheer van beveiligingsincidenten – BIO Hoofstuk 16

Doel:

Het kenbaar maken van informatiebeveiligingsincidenten zodat tijdig corrigerende maatregelen kunnen worden genomen.

Informatiebeveiligingsincidenten zijn alle gebeurtenissen die inbreuk maken op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en bijbehorende processen. De Kempenorganisaties hebben een incident management-proces ingericht. Dit omvat tenminste het registreren, classificeren en prioriteren, onderzoeken en analyseren, oplossen en reviewen van incidenten.

7.2.13 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer – BIO Hoofdstuk 17

Doel:

Het voorkomen van verstoringen in de IT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van calamiteiten.

De Kempenorganisaties zijn zodanig ingericht dat de continuïteit van de belangrijkste processen voldoende gewaarborgd wordt.

7.14 Naleving – BIO Hoofdstuk 18

Doel:

Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving en waarborgen dat systemen en processen voldoen aan het beveiligingsbeleid van de organisatie.

De Kempenorganisaties werken op basis van risicomanagement met een ISMS als ondersteunend instrument.

Vastgesteld in de vergadering van het Dagelijks Bestuur van De Samenwerking Kempengemeenten op 09-12-2025,

drs. W.A.C.M. Wouters
voorzitter

T.A.W.A. Pulles MPM
Directeur

Bijlage 1 Begrippenlijst

Applicatie	Een applicatie is software die bedoeld is voor computers of mobiele apparaten zoals smartphones, tablets en smartwatches.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en IT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een IT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid / Continuïteit	Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, bedrijfscontinuïteitsbeheer, ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Informatiebeveiligingsincidenten zijn alle gebeurtenissen die inbreuk maken op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en bijbehorende processen.
Baseline Informatiebeveiliging Overheid 2 (BIO)	De BIO2 is het normenkader voor informatiebeveiliging binnen de overheid, lees Rijksdienst, Provincie, Waterschappen, Gemeentes. De BIO2 kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staat de organisatie en de verantwoording over informatiebeveiliging binnen de Kempenorganisaties. De BIO2 bevordert de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie(systemen). Deze BIO2 is een richtlijn die een totaalpakket aan informatiebeveiligingscontrols en –maatregelen omvat die voor iedere organisatie noodzakelijk is om te implementeren.
Classificatie	Systematische identificatie en/of ordening van bedrijfsactiviteiten en/of records in categorieën overeenkomstig logisch gestructureerde afspraken, methodieken en procedurele voorschriften.
Cloud (applicatie)	Cloud is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van software (waaronder applicaties) en gegevens, buiten de eigen infrastructuur.
ENSIA	Eenduidige Normatiek Single Information Audit is een systematiek om verschillende informatiebeveiligingsonderdelen in audits en zelfevaluaties samen te voegen.
Gegeven	Weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat. Gegevens op zich behoeven niet noodzakelijkerwijs te zijn vastgelegd.
Governance	Stelsel van regels met betrekking op goed bestuur, toezicht en verantwoording. Betrokkenen dienen zich, los van vastgestelde regels, te houden aan toepasselijke waarden en normen.
Hardware	Dit is een verzamelnaam voor alle fysieke onderdelen die samenhangen met het computersysteem, zoals de computer zelf, de servers, het fysieke netwerk, de monitor, de printer en de modem.
IT-voorzieningen	Applicaties en technische infrastructuur waarop deze applicaties zijn geïnstalleerd.
Informatie	Betekenisvolle gegevens verzameld en uitgewerkt om te dienen als communicatie tussen personen. Informatie behoeft evenmin als gegevens noodzakelijkerwijs te zijn vastgelegd.
Informatiebeheer	1- Het systematisch verzamelen, verwerken, toegankelijk maken, gebruiken, onderhouden en verwijderen van informatie, opdat deze duurzaam toegankelijk en betrouwbaar is. De informatiebeheerder ondersteunt de gebruiker, die informatie creëert en raadpleegt.

	1- De inrichting en uitvoering van het opslaan, het bewaren en beheren, het ontsluiten of (actief) leveren, en waar nodig, het overdragen, verplaatsen, verwijderen of vernietigen van informatie.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Information Security Management System (ISMS)	In een ISMS worden alle werkzaamheden, besluiten, risico's en maatregelen beschreven.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Integriteit / betrouwbaarheid	Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. 1- Informatie is betrouwbaar als zij authentiek en volledig is. 2- Een record is betrouwbaar als de inhoud kan worden vertrouwd als een volledige en nauwkeurige weergave van de transacties, activiteiten of feiten waarvan het getuigt en waarop men zich kan verlaten bij de uitvoering van latere transacties of activiteiten.
IT-infrastructuur	Dit is de fysieke verkeersinfrastructuur ten behoeve van het transport van digitale data, met als hoger doel informatie te delen of aan te bieden en te consumeren.
Planning en Control	Planning en control omvat „strategic planning“, „management control“ en „task control“. Het is het proces van besluitvorming over - het bereiken van - de strategische doelen van de organisatie, het toedelen van taken aan leden van een organisatie om deze strategie te implementeren en het waarborgen dat de taken effectief en efficiënt worden uitgevoerd. NB. Control is niet hetzelfde als controle!
Software	Programma's die een computer (of ander apparaat) een bepaalde taak laten vervullen zoals spelletjes, tekstverwerker, webbrowser, etc.
Technische infrastructuur	Het deel van de IT-infrastructuur dat is gericht op de exploitatie van de systemen (hardware, systeemsoftware, bijbehorende documentatie, etc.). Samen met de applicatiesoftware en de bijbehorende documentatie en procedures vormt dit de IT- infrastructuur
Toegankelijk	Informatie is toegankelijk als deze vindbaar, interpreteerbaar en uitwisselbaar is voor daartoe bevoegde personen of systemen.
Vertrouwelijkheid / Exclusiviteit	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
Volledig	Informatie met betrekking tot een proces is volledig als alle informatie is vastgelegd en wordt beheerd die aanwezig zou moeten zijn conform het beheerregime dat voor dat proces is vastgesteld.

Bijlage 2 Rollen en verantwoordelijkheden

Gemeenteraad

De gemeenteraad stelt middelen beschikbaar voor informatiebeveiliging. Daarnaast heeft de gemeenteraad een controlerende functie ten aanzien van de informatiebeveiliging.

College van Burgemeester & Wethouders / Dagelijks Bestuur

Het college van B&W / DB is eindverantwoordelijk voor de adequate beveiliging van informatie binnen de gemeente. Eén lid van het college heeft informatiebeveiliging expliciet in de portefeuille. Het is de verantwoordelijkheid van het college om dit proces te faciliteren door:

- het informatiebeveiligingsbeleid vast te stellen;
- ervoor te zorgen dat voldoende middelen beschikbaar gesteld worden voor de adequate inrichting van informatiebeveiliging;
- toezicht te houden op de uitvoering van het informatiebeveiligingsbeleid;

MT (lijnmanagement)

Het MT is in haar sturende rol verantwoordelijk de uitvoering van het informatiebeveiligingsbeleid. Eén lid van het MT heeft informatiebeveiliging expliciet in het takenpakket. Het MT zorgt ervoor dat zij:

- stuurt op bedrijfsrisico's;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- toezicht houdt op de uitvoering van het informatiebeveiligingsplan;
- een positieve en actieve houding heeft ten aanzien van informatiebeveiliging;
- zorg draagt dat de medewerkers voldoende security training krijgen om de taken goed te kunnen uitvoeren;
- fungeert als voorbeeld richting de medewerkers.

Chief Information Security Officer (Informatiebeveiligingsfunctionaris)

De CISO is verantwoordelijk voor de organisatie van informatiebeveiliging. Dit is een rol op strategisch niveau binnen de gemeentelijke organisatie. De CISO heeft als taak informatiebeveiliging op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. De taken van de CISO ten aanzien van informatiebeveiliging zijn als volgt samen te vatten:

- Beleid & Coördinatie
- Controle & Registratie
- Communicatie & Voorlichting
- Advies & Rapportage

Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) houdt zich bezig met alle privacyaspecten binnen de Kempenorganisaties. De functie is onafhankelijk van de lijn belegd en de functionaris heeft de bevoegdheid om rechtstreeks naar de gemeentesecretaris, het college van B&W, de directeur of het Dagelijks bestuur van de gemeenschappelijke regeling te rapporteren. De taken van de FG zijn:

- adviseren (zowel gevraagd als ongevraagd) over vraagstukken die te maken hebben met de omgang met persoonsgegevens;
- toezien op de naleving van de AVG en andere privacy-gerelateerde wet- en regelgeving binnen de organisatie;
- het informeren van de organisatie betreffende de AVG en andere privacy-gerelateerde wet- en regelgeving;
- het zijn van een contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn)
- m.b.t. de omgang met persoonsgegevens. De FG is daarbij gehouden aan geheimhouding;
- het coördineren van de afhandeling van datalekken conform de vastgestelde datalekprocedure;
- het contactpunt met de Autoriteit Persoonsgegevens.

Privacy Officer

De Privacy Officer is verantwoordelijk voor de uitvoering en naleving van de privacywetgeving. Daarnaast adviseert de Privacy Officer over privacybescherming en activiteiten ter bescherming van persoonsgegevens.

Beveiligingsfunctionaris Burgerzaken

De beveiligingsfunctionaris is bevoegd om een jaarlijks intern onderzoek in te stellen naar de werking van de beveiligingsprocedures ten aanzien van reisdocumenten en rijbewijzen. Het college van B&W krijgt inzicht in de rapportage van bevindingen.

Security Officer Suwinet

De Security Officer Suwinet is binnen de organisatie toezichthouder betreft het proces rondom informatiebeveiliging binnen het Suwinetdomein en rapporteert direct aan het DB (zie ook aansluitbeleid Suwinet).

Proceseigenaren

De proceseigenaar gaat over de inrichting, het ontwerp en de resultaten van het proces. Hiervoor dient de proceseigenaar het proces te analyseren, risico's in kaart te brengen en passende maatregelen te treffen. Proceseigenaren informeren het lijnmanagement en de directie zodat zij beslissingen kunnen nemen ten aanzien van informatiebeveiliging.

Technisch applicatiebeheerder

De technisch applicatiebeheerder is verantwoordelijk voor het inrichten en in stand houden van de programmatuur.

Functioneel beheerder

De functioneel beheerder zorgt ervoor dat de applicatie is ingericht conform de daarvoor gestelde eisen en richtlijnen. De functioneel beheerder is verantwoordelijk voor het onderhouden van de programmatuur en het inregelen van de juiste autorisaties binnen de applicatie.

Gegevensbeheerder

De gegevensbeheerder is in een of meerdere informatiesystemen verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

Het Shared Service Center (GRSK-SSC)

Het SSC beheert de werkplekken, server platformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings-)beheer van databases, bedrijfsapplicaties en kantoorautomatisering hulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie-)systemen afgelegd. Namens SSC sluit de beveiligingsbeheerder IT aan bij het informatieveiligheidsoverleg.

Facilitaire zaken

Facilitaire Zaken is lokaal geregeld (elke vestiging heeft een eigen facilitair beheerder). Zij zijn verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting.

Personeelszaken

Personeelszaken is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.