Kempen gemeenten

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1272

22 december 2020

Officiële uitgave van de gemeenschappelijke regeling Samenwerking Kempengemeenten

Beleidsregel informatiebeveiligingsbeleid Kempengemeenten, GRSK en KempenPlus 2020

het Dagelijks Bestuur van de Gemeenschappelijke Regeling Samenwerking Kempengemeenten

gelet op het artikel 4:81 van de Algemene wet bestuursrecht;

b e s l u i t

vast te stellen de volgende beleidsregel:

Beleidsregel informatiebeveiligingsbeleid Kempengemeenten, Gemeenschappelijke Regeling Samenwerking Kempengemeenten en KempenPlus 2020

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, de Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK) en de Gemeenschappelijke Regeling Participatiebedrijf Kempenplus (KempenPlus) 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 Kempengemeenten, de Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK) en de Gemeenschappelijke Regeling Participatiebedrijf KempenPlus (KempenPlus) om informatie op een passende wijze te beveiligen.
Dit informatiebeveiligingsbeleid vervangt het 'Informatieveiligheidsbeleid Kempengemeenten en de Gemeenschappelijke Regeling Samenwerking Kempengemeenten 2018'.
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 gemeente in de meest brede zin van het woord.
Belangrijke uitgangspunten hierbij zijn:

- Informatiebeveiliging is en blijft een verantwoordelijkheid van de hele organisatie. Voor de gemeenten 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 gemeente ten aanzien van informatiebeveiliging en hoe ervoor gezorgd kan worden dat informatiebeveiliging geborgd blijft binnen de gemeente.
In het beleid is een groeimodel aangegeven waar de Kempengemeenten 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 gemeenten, GRSK en KempenPlus 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 gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan vertrouwelijke (persoons-)gegevens van inwoners en bedrijven. Daarnaast zijn gemeenten verantwoordelijk voor een betrouwbare en continue

dienstverlening. Onze inwoners vertrouwen erop dat de gemeente haar vertrouwelijke gegevens afdoende beveiligt. Het is daarom belangrijk dat informatie op passende wijze beveiligd wordt.

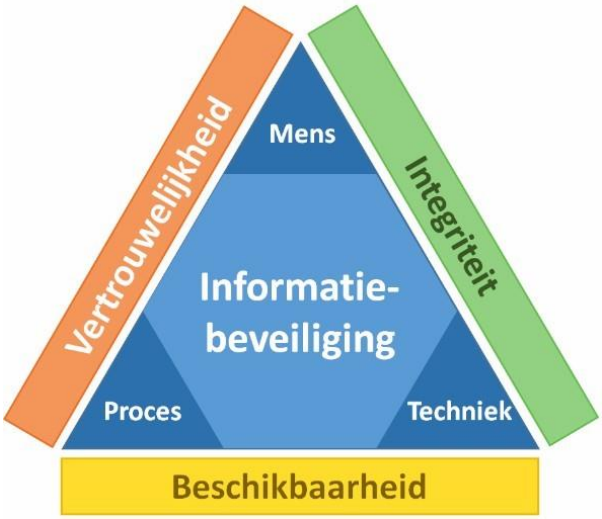
1.1 Doelstelling

Het doel van dit beleid is het vastleggen van algemene beleidsuitgangspunten over informatiebeveiliging voor de Kempengemeenten, Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK) en Gemeenschappelijke Regeling Participatiebedrijf KempenPlus (KempenPlus). Het beleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). 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 en Gemeenschappelijke Regeling Samenwerking Kempengemeenten 2018'.

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 gemeente verstaat 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 gemeenten 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 uitingsvormen 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 gemeenten 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 en Suwi. 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.

3. Kaders & uitgangspunten

3.1 Kader

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 gemeente. 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 Kempengemeenten 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 gemeente legt jaarlijks verantwoording af over haar informatiebeveiliging via de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit).
- 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 gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen 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 Kempengemeenten 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 gemeente als haar inwoners. Een belangrijke ontwikkeling is dat de Kempengemeenten 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 keten-partners. Het netwerk van informatie-uitwisseling ontwikkelt zich nog steeds. Met het stelsel van basisregistraties krijgt de gemeente ook steeds breder toegang tot landelijke gegevensvoorzieningen. Informatie is een cruciaal bedrijfsmiddel voor gemeenten.

Vanwege het cruciale belang van informatie voor gemeenten, 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 gemeente.

4.2 Visie

Een betrouwbare informatievoorziening is noodzakelijk voor het functioneren van de gemeentelijke organisatie. De gemeente beveiligt haar systemen en processen om uitval van vitale processen en dienstverlening te voorkomen. Daarnaast is het de plicht van de gemeente 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 gemeente hanteert 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 gemeenten. De Kempengemeenten streven de volgende doelen na om een adequaat niveau van beveiliging conform de Baseline Informatiebeveiliging Overheid (BIO) en aanverwante wet- en regelgeving te bereiken:

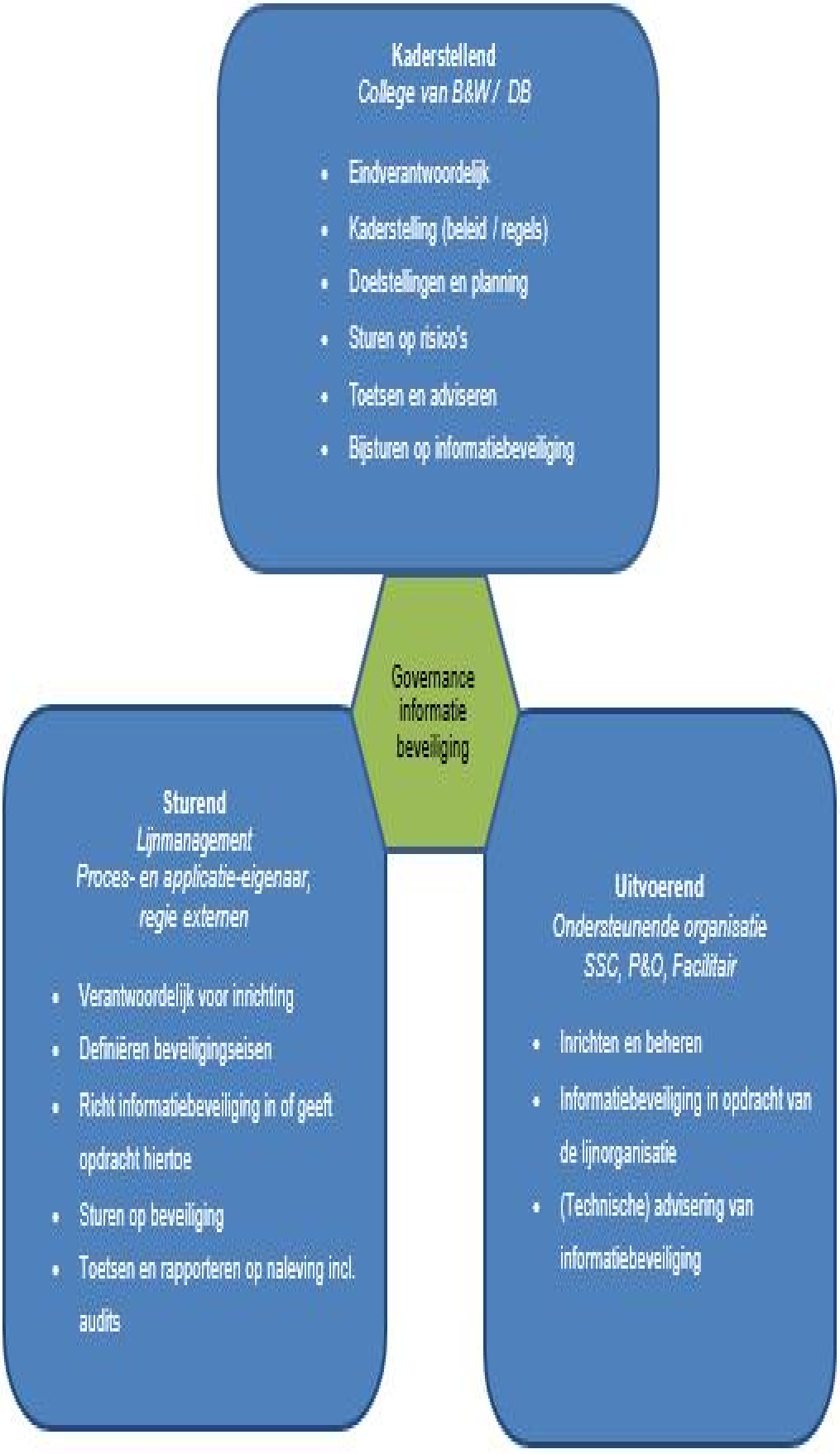
1. De Kempengemeenten borgen de beveiligingseisen (controls) volgens de BIO door implementatie van aan de control gerelateerde informatiebeveiligingsmaatregelen.
2. De Kempengemeenten zijn 'in control' over de geïmplementeerde informatiebeveiligingsmaatregelen, middels verankering in een PDCA-cyclus.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


Kaderstellend
College van B&W / DB
Eindverantwoordelijk
Kaderstelling (beleid / regels)
Doelstellingen en planning
Sturen op risico's
Toetsen en adviseren
Bijsturen op informatiebeveiliging
Governance informatie beveiliging
Sturend
Lijnmanagement
Proces- en applicatie-eigenaar, regie externen
Verantwoordelijk voor inrichting
Definiëren beveiligingseisen
Richt informatiebeveiliging in of geeft opdracht hiertoe
Sturen op beveiliging
Toetsen en rapporteren op naleving incl. audits
Uitvoerend
Ondersteunende organisatie
SSC, P&O, Facilitair
Inrichten en beheren
Informatiebeveiliging in opdracht van de lijnorganisatie
(Technische) advisering van informatiebeveiliging

5.1.1 Kaderstellend
De directie (College van B&W / DB) is vanuit haar sturende rol eindverantwoordelijk voor de informatiebeveiliging. Door middel van het vaststellen van dit informatiebeveiligingsbeleid stellen zij de kaders vast waarmee informatiebeveiliging voor de Kempengemeenten vormgegeven wordt. De directie houdt toezicht op de naleving van het beleid en laat zich hier gevraagd en ongevraagd over informeren, teneinde zich te kunnen verantwoorden aan de raad over informatiebeveiliging.

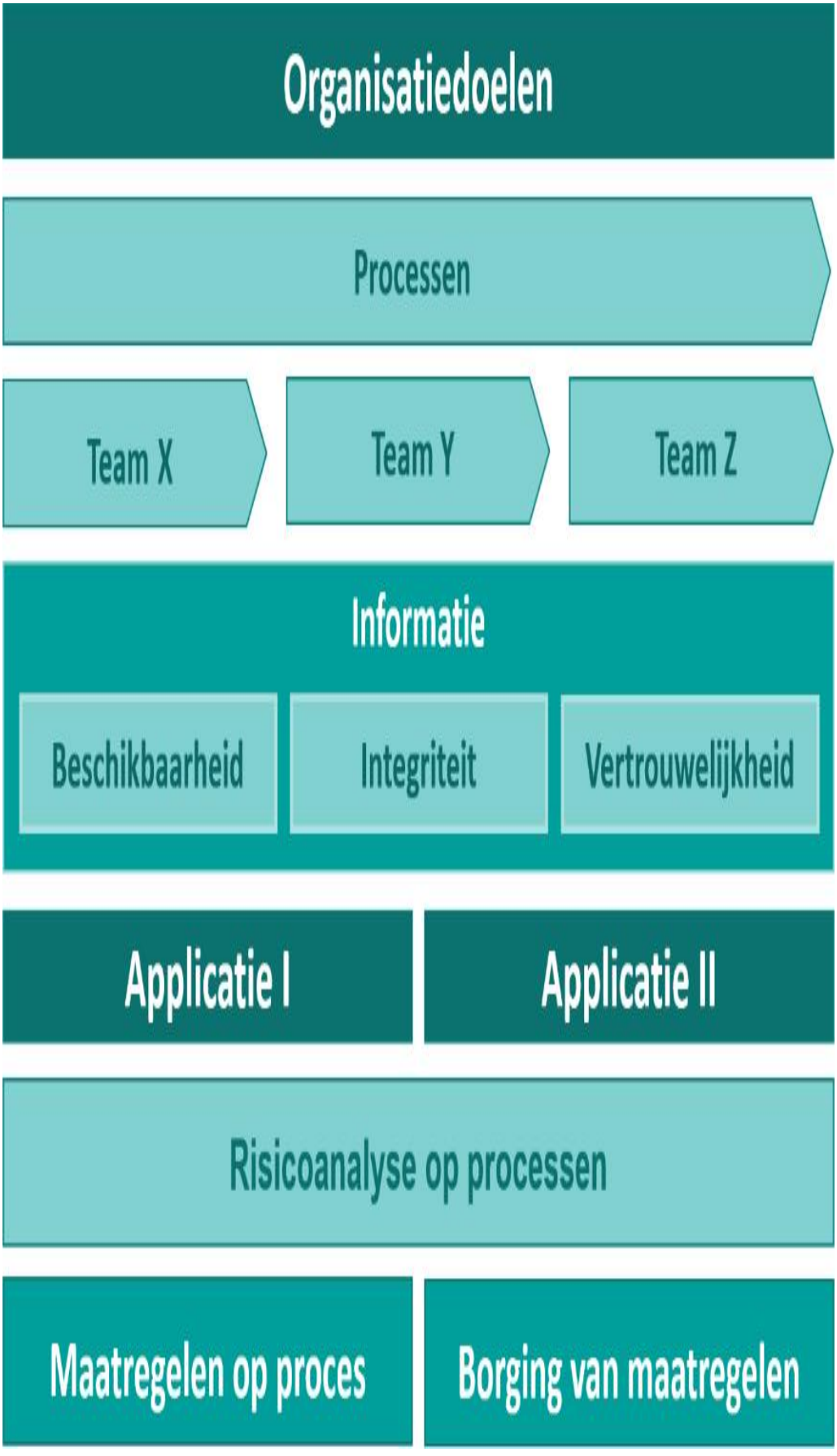
5.1.2 Sturend
Het management is verantwoordelijk voor sturing op de uitvoering van informatiebeveiliging. Zij sturen op de uitvoering van het informatiebeveiligingsbeleid en dragen dit uit naar de organisatie. Op basis van risicomanagement worden afwegingen gemaakt voor een juist beveiligingsniveau. Het management wijst proces- en applicatieverantwoordelijken aan. De proces en applicatieverantwoordelijken treffen de juiste maatregelen om de informatiebeveiliging op het gekozen niveau te waarborgen.

5.1.3 Uitvoerend
De ondersteunende organisatie is verantwoordelijk voor de uitvoering van informatiebeveiliging. Elke medewerker is verantwoordelijk om de informatie binnen de processen op een juiste manier te beveiligen. Vanuit de functie kan een medewerker specifieke verantwoordelijkheden voor informatiebeveiliging hebben.

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. Het bestuur van de Kempengemeenten is verantwoordelijk voor de borging van dit informatiebeveiligingsbeleid en de controle hierop.
De gemeenten verantwoorden zich jaarlijks over hun informatiebeveiliging middels de ENSIA-systematiek. De verantwoording over de informatiebeveiliging komt tot uitdrukking in het jaarverslag van de gemeenten en de verschillende beveiligingsrapportages die volgen uit ENSIA. Op basis van de rapportages worden verbetermaatregelen geformuleerd en opgenomen in het informatiebeveiligingsplan.

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 gemeenten aantoonbaar grip houden op de veiligheid.


Organisatiedoelen
Processen
Team X
Team Y
Team Z
Informatie
Beschikbaarheid
Integriteit
Vertrouwelijkheid
Applicatie I
Applicatie II
Risicoanalyse op processen
Maatregelen op proces
Borging van maatregelen

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 Kempengemeenten 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 gemeenten 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: risico = kans x 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 beveiligingseisen 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 gemeente hier een geaccepteerd risico loopt. Tegelijkertijd houdt dit in dat mogelijk meer maatregelen getroffen moeten worden ten opzichte van de baseline indien de gemeente een hoog risico loopt. Op deze wijze worden tijd, geld en middelen passend besteed met als gevolg een stelsel van beveiligingsmaatregelen dat bij de gemeenten 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 gemeente tenminste dient 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 Kempengemeenten 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

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, informatiesystemen 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 gemeenten 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 gemeenten borgen de onweerlegbaarheid van verzending, ontvangst berichtenuitwisseling en het vertrouwd opslaan van bestanden. Hiervoor treffen de gemeenten 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 gemeenten 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 gemeenten 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 gemeente en andere organisaties of inwoners;
- (cloud-)applicaties van de gemeente die extern van de gemeentelijke IT-infrastructuur opereren.

Op deze wijze wordt geborgd dat de gemeenten 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 gemeenten 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 Hoofdstuk. 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 gemeenten 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 gemeenten 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 gemeenten werken op basis van risicomanagement met een ISMS als ondersteunend instrument.

8 Intrekking oude beleidsregel

De beleidsregel Informatiebeveiligingsbeleid Kempengemeenten en Gemeenschappelijke Regeling Kempengemeenten 2018 wordt ingetrokken.

9 Inwerkingtreding en citeertitel

1. Deze beleidsregel treedt in werking op de dag na de bekendmaking.
2. Deze beleidsregel wordt aangehaald als: Beleidsregel informatiebeveiligingsbeleid Kempengemeenten, GRSK en KempenPlus 2020.

Aldus vastgesteld door het Dagelijks Bestuur van de GRSK
op 23 juni 2020
de voorzitter, mevrouw A. Callewaert - de Groot
de directeur, de heer B. Cerutti