Kampen

# GEMEENTEBLAD

Officiële uitgave van de gemeente Kampen

Nr. 524791

9 december

2025

## Strategisch Informatiebeveiligings- en privacybeleid gemeente Kampen

Het college van burgemeester en wethouders;
gelezen het voorstel van 11 juni 2024, kenmerk 42119-2024;
gelet op artikel 5.1 van de Baseline Informatiebeveiliging Overheid en artikel 24 lid 2 van de Algemene verordening gegevensbescherming;
besluit vast te stellen de volgende regeling:
**Strategisch Informatiebeveiligings- en privacybeleid gemeente Kampen**

### 1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacybeleid van de gemeente Kampen. Het is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

De beleidsnota sluit aan bij de ambities van het college om goed in verbinding te staan met inwoners, ondernemers en samenwerkingspartners om optimale (digitale) dienstverlening te bieden. We werken met veilige digitale systemen en benutten de techniek verantwoord. Met behulp van data kunnen we leren en verbeteren. Zo streven we naar een steeds betere (digitale) dienstverlening.

| |
|---|
| Doelstelling:<br>Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.<br><br>Resultaat:<br>Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid en privacy alsmede het vereiste ambitieniveau zijn vastgelegd.<br><br>Wat merken inwoners, bedrijven en ketenpartners van dit beleid:<br>Informatie is een belangrijk bedrijfsmiddel. Beveiliging van deze informatie is nodig om een goede en veilige dienstverlening naar inwoners, bedrijven en ketenpartners te garanderen. De gemeente Kampen is een betrouwbare partner voor al haar inwoners, bedrijven en ketenpartners. |

Met dit strategisch beleid zet de gemeente Kampen een volgende stap om de beveiliging van (persoons)gegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid zijn de ISO 27001 en 27002 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (hierna: BIO) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de Vereniging van Nederlandse Gemeenten (hierna: VNG) en de beginselen uit de Algemene verordening gegevensbescherming (hierna: AVG) voor het verwerken van persoonsgegevens.

Dit strategische beleid is een uitwerking van de paragraaf Informatieveiligheid in het Beleidsplan Dienstverlening en informatie. Dit beleid wordt jaarlijks geëvalueerd en zonodig geactualiseerd.

#### 1.1. Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen en door directie vast te stellen ‘Gemeentelijk Informatiebeveiligings- en privacyplan’ (hierna: jaarplan) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie zijn belegd.

Deze beleidsnota brengt niet (geheel) de huidige situatie in beeld, maar beschrijft het ambitieniveau. De acties om tot dit ambitieniveau te komen worden opgenomen in separaat op te stellen jaarplannen.

### 1.2. 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.

Dit strategisch beleid geldt voor alle informatiebeveiliging gerelateerde processen van de gemeente Kampen en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

### 1.3. Privacy & Gegevensbescherming (AVG)
De gemeente Kampen werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens worden verzameld voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken voor het sociaal domein, burgerzaken, openbare orde en het veiligheidsdomein. Om als gemeente deze taken goed uit te voeren, zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

### 1.4. Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy
De komende jaren pakt de gemeente Kampen door op het verhogen en waarborgen van informatieveiligheid en privacy in de organisatie. Dat vereist een integrale aanpak, goed opdrachtgeverschap, onderlinge samenwerking en risicobewustzijn waarbij iedere afdeling betrokken is. De nadruk komt hierdoor te liggen op de governance rond informatiebeveiliging. Ook de BIO haakt hierop in door de verantwoordelijkheid voor informatiebeveiliging en een veilige omgang met gegevens in de organisatie nadrukkelijk neer te leggen bij het bestuur en proceseigenaren. Deze verantwoordelijkheid moet ervoor zorgen dat de risico's op het niveau van werkprocessen en informatiesystemen in beeld zijn en dat daar passende beveiligingsmaatregelen voor genomen worden. Risicomanagement wordt hiervoor als middel ingezet. Ook het periodiek afleggen van verantwoording over de risicoafweging en over de effectieve werking van beveiligingsmaatregelen aan de gemeenteraad komt nadrukkelijk te liggen bij het bestuur en de proceseigenaren en is mede van belang voor het gestelde vertrouwen in de ketensamenwerking binnen de overheid en ketenpartners.

## 2. Strategisch beleid

### 2.1. Doel
Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligings- en privacybeleid'. De uitwerking van dit beleid is opgenomen in het jaarplan door middel van concrete maatregelen en activiteiten. Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

### 2.2. Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het strategisch beleid worden in de volgende paragrafen benoemd.

#### *2.2.1. De BIO*
De BIO is het normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat het management nu meer dan vroeger moet werken volgens de aanpak van de ISO 27001 en 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 zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

#### *2.2.2. De AVG*

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Kampen is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de AVG.

***2.2.3. De Wpg***
De gemeente Kampen heeft boa's in dienst en zij verwerken naast persoonsgegevens die onder de AVG vallen ook politiegegevens die onder de Wet Politiegegevens (hierna: Wpg) vallen. Voor de verwerking van deze politiegegevens moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op onder andere toegangsrechten, autorisaties, data-classificatie, risico-inschatting, registratie, logging, meldplicht en documentatieplicht.

***2.2.4. De 10 principes voor informatiebeveiliging***
De 10 principes voor informatiebeveiliging – zoals de VNG deze voorschrijft – zijn een bestuurlijke aanvulling op de BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Deze principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Verdere toelichting op de principes is opgenomen in bijlage 2. De principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente Kampen. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Naast de 10 principes van informatiebeveiliging hanteert de gemeente Kampen ook strategische doelen, deze worden behandeld in paragraaf 2.6.1.

***2.2.5. Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten***
Het door de Informatie Beveiligingsdienst (IBD) periodiek opgestelde 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 zeer geschikt om focus aan te brengen in het actualiseren van (tactisch) beleid.

In het Dreigingsbeeld 2023-2024 ziet de IBD drie soorten dreigingen opvallen:
- Meer ransomware met destructievere gevolgen.
- Steeds meer en ernstiger kwetsbaarheden in software.
- Gevaren in ketens uit het zicht.

Voor het vergroten van de weerbaarheid van gemeenten ziet de IBD zes succesfactoren:
- Financiën: reserveer een vast percentage in het budget voor informatiebeveiliging en privacy.
- Techniek: de basismaatregelen tegen ransomware zijn op orde.
- Eigenaarschap management: informatiemanagement en gegevensbescherming staan op de managementagenda.
- Organisatie: positie Chief Information Security Officer (CISO) en een veilige cultuur.
- Samenwerkingsverbanden: maak afspraken en zie er op toe.
- Factor mens: investeren in bewustwording.

***2.2.6. Informatie uit incidenten, inbreuken op de beveiliging en datalekken***
De gemeente Kampen kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijke input bij het actualiseren van het beleid.

## 2.3. Kader en standaarden informatiebeveiliging

De basis voor de inrichting van dit strategisch beleid zijn de normen ISO 27001 en 27002. De gemeente Kampen neemt maatregelen in het kader van informatiebeveiliging op basis van best practices en de BIO. De BIO is een uitwerking van onder andere de normen ISO 27001 en 27002.

Naast de BIO richt dit strategisch beleid zich ook op de Cybersecurity Implementatie Richtlijn (hierna: CSIR). Binnen de gemeente Kampen wordt naast ICT ook operationele technologie ingezet. Operationele technologie is een verzamelnaam voor systemen die apparaten besturen middels procesautomatisering. De gemeente Kampen gebruikt de CSIR als richtlijn ter bescherming voor procesautomatisering.

Naast het bovengenoemde kader toetst de gemeente Kampen middels dataclassificatie (zie bijlage 3) de beschikbaarheid, integriteit en betrouwbaarheid van haar informatie(systemen).

## 2.4. Scope informatiebeveiliging en privacy

De scope van deze beleidsnota omvat de volgende onderdelen:

- Alle gemeentelijke processen met de onderliggende informatiesystemen;
- Procesautomatisering;
- Informatie en gegevens van de gemeente Kampen en externe partijen;
- Het gebruik van deze informatie en gegevens door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

## 2.5. Plaats van het strategisch beleid

Dit strategisch beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen af uit wetgeving als BIO, AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en Suwinet. Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen. Deze worden in aanvullende (tactische en operationele) beleidsdocumenten geformuleerd.

In onderstaand overzicht wordt de relatie weergegeven tussen het strategische beleid en een niet-uitputtende lijst van onderhevige beleidsdocumenten.


## 2.6. Uitgangspunten

Het bestuur en het management spelen een cruciale rol bij het uitvoeren van het strategisch beleid. Het management maakt een inschatting van het belang die de verschillende delen van de informatievoorziening voor de gemeente hebben, de (privacy)risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van het beleid van en voor de hele gemeente. Het beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

### *2.6.1. Strategische doelen*

De strategische doelen van het beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.

- 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.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de BIO, AVG en Wpg en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

***2.6.2. Belangrijkste uitgangspunten***

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Kampen hebben een interne eigenaar die de vertrouwelijkheid, privacyregels en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie is de kwaliteit van de informatiebeveiliging en privacy verankerd binnen de organisatie. Het strategisch beleid vormt samen met het jaarplan het fundament onder een betrouwbare informatievoorziening en privacybescherming. In het jaarplan wordt de betrouwbaarheid van de informatievoorziening, -beveiliging en privacy organisatiebreed benaderd. Het jaarplan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacyregels volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het strategisch beleid worden vastgelegd en vastgesteld.
- 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.
- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

***2.6.3. IB&P- governance***

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college stelt als eindverantwoordelijke voor informatiebeveiliging en privacyveiligheid het strategisch beleid vast.
- De directie stelt jaarlijks het jaarplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken, vaststellen en uitvoeren van onderwerp specifieke tactische en operationele beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid vallen.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de Planning & Control-gesprekken (hierna: P&C-gesprekken).
- De Information Security Officer (ISO) ondersteunt de CISO. De ISO is op tactisch niveau verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's en het opstellen van rapportages.

- De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college over de juiste en zorgvuldige omgang met persoonsgegevens, zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen inzake de verwerking van persoonsgegevens vastlegt.
- De Privacy Officer (PO) is belast met de uitvoering en de naleving van de AVG. Daarnaast adviseert de PO over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
- De concerncontroller is verantwoordelijk voor het verbijzonderde toezicht op de naleving van beleid op het gebied van informatiebeveiliging en privacy.
- De directie en de afdelingshoofden stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de FG.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy naar aanleiding van de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingshoofden zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De afdelingshoofden zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen de processen rondom deze registraties niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering en rondom de registraties zijn belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Afdelingshoofden dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens hebben ingezien en verwerkt.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden voeren quickscans informatiebeveiliging uit op basis van de BIO. Tevens voeren zij bij het verwerken van persoonsgegevens (pre-)DPIA's uit op basis van de AVG om risicoafwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maken deel uit van de beoordelingssystematiek en worden besproken tussen het afdelingshoofd en de medewerker.

2.6.4. Randvoorwaarden

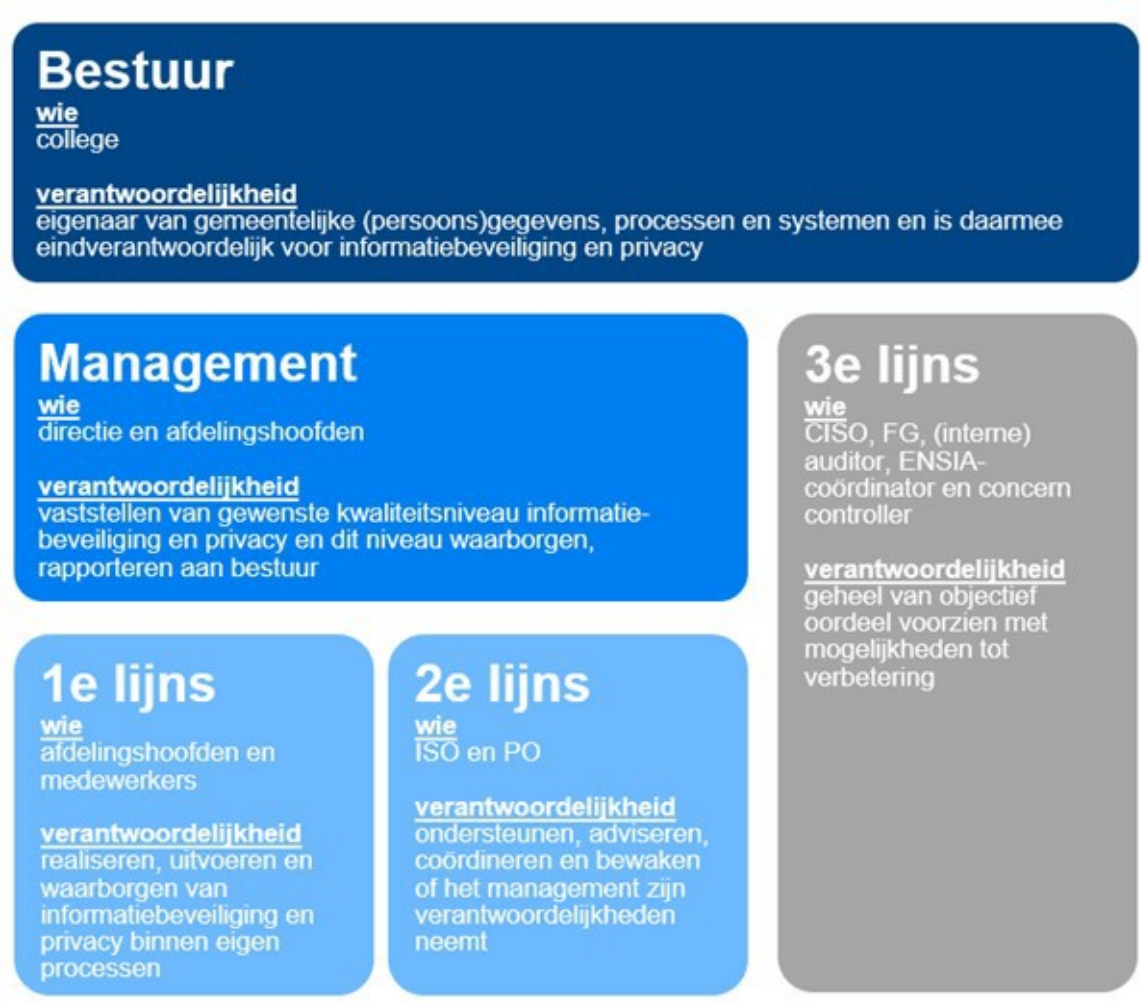
Belangrijke randvoorwaarden zijn:

- De eisen rondom informatiebeveiliging en privacybescherming maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacy en omgang met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een jaarplan opgesteld onder leiding van de CISO, gebaseerd op:
    - Dit strategisch beleid;
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Andere audit resultaten;
    - Het dreigingsbeeld gemeenten van de IBD;
    - Uitkomsten risicoanalyses en DPIA's;
    - De door de afdelingshoofden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een DPIA.

- Om uitvoering te kunnen geven aan dit strategisch beleid en het jaarplan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

## 3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. Hieronder worden deze rollen en verantwoordelijkheden overzichtelijk weergegeven.




### 3.1. Rollen en verantwoordelijkheden op niveau

#### *3.1.1. Bestuur*

*Gemeenteraad*

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente Kampen, zo ook voor informatiebeveiliging en privacy. Het college legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de gemeenteraad over de stand van zaken van informatiebeveiliging ten opzichte van het in dit beleid vastgestelde kader.

*College*

Het college is eigenaar van de gemeentelijke informatieprocessen en -systemen en draagt hiermee de eindverantwoordelijkheid voor een passend niveau van informatiebeveiliging en privacy. Hierbij neemt het college de 10 principes voor informatiebeveiliging in acht die door de VNG zijn geformuleerd (zie paragraaf 2.2.4). Verder stelt het college met deze beleidsnota de kaders ten aanzien van informatiebeveiliging en privacy op basis van landelijke en Europese wet- en regelgeving vast. Het college informeert de gemeenteraad over de informatiebeveiliging van de gemeente door dit op te nemen in de jaarrekening van de gemeente. Hierin wordt de gemeenteraad op de hoogte gebracht van de stand van zaken, de uitgevoerde plannen van het afgelopen jaar, de tijdsplanning en de plannen voor het volgende jaar.

#### *3.1.2. Management*

*Directie*
De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directie zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging en bescherming van de privacy van (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacy een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de gemeenteraad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor (laten) uitwerken, vaststellen en uitvoeren van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de ISO en PO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. De onderwerpen informatiebeveiliging en privacy worden in de gemeente Kampen gezien als een integraal onderdeel van risicomanagement.

*Afdelingshoofden*
Het toepassen en waarborgen van informatiebeveiliging en privacy vallen onder de verantwoordelijkheid van alle afdelingshoofden. Om deze verantwoordelijkheid waar te maken, dienen zij goed ondersteund te worden vanuit de eerste (medewerkers) en tweede lijn. De bedoeling is dat alle processen, systemen, (persoons)gegevens en applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

#### *3.1.3. 1e lijns*
*Afdelingshoofden*
Naast de hierboven genoemde verantwoordelijkheden hebben de afdelingshoofden ook taken in het kader van informatiebeveiliging en privacy die zij uitvoeren vanuit de eerste lijn. Deze taken zijn:
- Het rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde activiteiten op het gebied van informatiebeveiliging en privacy.
- Het afstemmen met de afdelingen over de inhoudelijke aanpak over informatiebeveiliging en privacy. Deze afstemming vindt minimaal twee keer per jaar plaats tijdens het bedrijfsvoeringsoverleg.
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing zijn en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht zijn.
- Het binnen de eigen afdeling uitdragen van het IB&P-beleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO, ISO en PO bij nieuwe of gewijzigde processen.
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die hieruit voortvloeien voor beleid en maatregelen.

*Medewerkers*
Medewerkers moeten zorgvuldig en gedisciplineerd omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit, de beschikbaarheid en de controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken. In het tactisch beleid zijn gedragsregels in het kader van informatiebeveiliging uitgewerkt. Iedere medewerker wordt geacht deze gedragsregels te kennen en deze uit te dragen.

#### *3.1.4. 2e lijns*
*Information Security Officer (ISO)*
De ISO ondersteunt de CISO. De rol van ISO is op tactisch niveau verantwoordelijk voor het actueel houden van het tactisch informatieveiligheidsbeleid, het coördineren van de uitvoering van beleid op gebied van informatiebeveiliging, het adviseren bij projecten en het beheersen van risico's.

*Privacy Officer (PO)*
De PO is belast met de uitvoering en de naleving van de AVG. Daarnaast adviseert de PO over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

#### *3.1.5. 3e lijns*
*Chief Information Security Officer (CISO)*
De CISO is op strategisch en organisatieniveau verantwoordelijk voor het actueel (laten) houden van het informatieveiligheidsbeleid, het (laten) coördineren van de uitvoering van het beleid, het beheersen

van risico's overeenkomstig de behoeften en de risicobereidheid van de organisatie, evenals het rapporteren aan het college en de directie.

*Functionaris gegevensbescherming (FG)*
De FG is conform de AVG de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente. Daarnaast rapporteert de FG rechtstreeks aan het college en de directie.

*Concerncontroller*
De concerncontroller is verantwoordelijk voor het verbijzonderde toezicht op de naleving van beleid op het gebied van informatiebeveiliging en privacy.

### 3.2. Controle en verantwoording

Het strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Kampen. De bestuurders en directeuren werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

#### *3.2.1. ENSIA*

De gemeente Kampen verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden leveren vervolgens alle informatie die nodig is voor het invullen van de ENSIA-vragenlijsten.

De verantwoording over informatiebeveiliging en privacy komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging en privacy. Met deze verklaring geeft het college aan in hoeverre de gemeente Kampen voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en voor de wettelijke eisen zoals genoemd in de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente Kampen gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de gemeenteraad.

Via ENSIA verantwoordt de gemeente Kampen zich ook aan de stelselhouders voor DIGID/WOZ/BAG/SUWI.

Middels deze verantwoording worden het bestuur en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Kampen informatiebeveiliging en privacy serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

## 4. Intrekking huidige beleid

Met invoering van het 'Strategisch Informatiebeveiligingsbeleid gemeente Kampen' wordt het voormalig geldende 'Informatiebeveiligingsbeleid Gemeente Kampen 2018-2021' ingetrokken.

## 5. Inwerkingtreding

Het besluit treedt in werking op de dag na de bekendmaking.

*Aldus vastgesteld door de directie namens het college van burgemeester en wethouders en de burgemeester op 18 juni 2024.*
*De directie van de gemeente Kampen,*
*N. Middelbos, secretaris*

## Bijlage 1: Afkortingenlijst

| | |
|---|---|
| AVG | Algemene verordening gegevensbescherming |
| BAG | Basisregistratie Adressen en Gebouwen |
| BGT | Basisregistratie Grootschalige Topografie |
| BIO | Baseline Informatiebeveiliging Overheid |
| BRP | Basisregistratie Personen |
| CISO | Chief Information Security Officer |
| CSIR | Cybersecurity Implementatie Richtlijn |
| DigiD | Digitale persoonsidentificatie |
| DPIA | Data protection impact assessment |
| ENSIA | Eenduidige Normatiek Single Information Audit |
| FG | Functionaris Gegevensbescherming |
| IBD | Informatie Beveiligingsdienst |
| IB&P-beleid | Strategisch Informatiebeveiligings- en privacybeleid gemeente Kampen 2023-2026 |
| IB&P-plan | Gemeentelijk Informatiebeveiligings- en privacyplan |
| ISO (norm) | Internationale Organisatie voor Standaardisatie |
| ISO (rol) | Information Security Officer |
| PO | Privacy Officer |
| PNIK/PUN | Wet- en regelgeving Reisdocumenten |
| Suwinet | Structuur uitvoeringsorganisatie Werk en Inkomen |
| UAVG | |
| VNG | Vereniging van Nederlandse Gemeenten |
| Wpg | Wet politiegegevens |

## Bijlage 2. De 10 bestuurlijke principes voor informatiebeveiliging

*Uit VNG Realisatie; 2019*

**1. Bestuurders bevorderen een veilige cultuur**

*Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.*

Zonder open cultuur waar iedereen vrij is om te spreken, is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

**2. Informatiebeveiliging is van iedereen**

*Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.*

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO) en Functionaris Gegevensbescherming (FG) als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

**3. Informatiebeveiliging is risicomanagement**

*Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.*

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

**4. Risicomanagement is onderdeel van de besluitvorming**

*Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache .*

U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

**5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking**

*Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.*

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

**6. Informatiebeveiliging is een proces**

*Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.*

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

**7. Informatiebeveiliging kost geld**

*Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.*

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieveen/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

**8. Onzekerheid dient te worden ingecalculeerd**

*De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.*

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

**9. Verbetering komt voort uit leren en ervaring**
*Risicobeheer wordt voortdurend verbeterd door leren en ervaring.*
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

**10. Het bestuur controleert en evalueert**
*Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.*
Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie Vereniging van Nederlandse Gemeenten 7 omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

**Bijlage 3. Tabel dataclassificatie**

| Niveau | Vertrouwelijkheid | Integriteit | Beschikbaarheid |
|---|---|---|---|
| **Geen / 0**<br><br>**(geen schade)** | **Openbaar**<br><br>Informatie mag door iedereen worden ingezien<br><br>*( bijv : algemene informatie op de website, openbaar gemaakte stukken)* | **Niet zeker**<br><br>Informatie mag worden veranderd, er zijn geen garanties m.b.t. de juistheid of volledigheid van de informatie<br><br>*( bijv : templates en sjablonen)* | **Niet nodig**<br><br>Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (MTD* meerdere weken)<br><br>*( bijv : ondersteunende tools als routeplanner)* |
| **Laag / I**<br><br>**(enige schade)** | **Bedrijfsvertrouwelijk**<br>Informatie die door alle medewerkers van de organisatie mag worden ingezien<br><br>*( bijv : informatie op het intranet, zakelijke contactgegevens van medewerkers)* | **Beschermd**<br>Onjuiste of onvolledige informatie heeft nauwelijks impact op processen, informatie moet hooguit opnieuw worden verzameld<br><br>*( bijv : interne (management) rapportages, verzamelde publieke informatie)* | **Belangrijk**<br>Informatie mag incidenteel niet beschikbaar zijn (MTD* 2 weken)<br><br>*( bijv : administratieve gegevens, zoals personeelsadministratie, factuurverwerking)* |
| **Midden / II**<br><br>**(serieuze schade)** | **Vertrouwelijk**<br>Informatie die door een kleine groep medewerkers (zoals een afdeling of een (project)team) mag worden ingezien, voor zover nodig voor hun taken<br><br>*( bijv : overige persoonsgegevens, BSN, aanbestedings -, handhavings-, en vergunningsinformatie, financiële procesgegevens, integriteitsprocedures, specifieke informatie over beveiliging)* | **Hoog**<br>Onjuiste of onvolledige informatie leidt tot verkeerde beslissingen en heeft impact op processen<br><br>*( bijv : salarisadministratie, primaire procesinformatie zoals vergunningen, handhavingsinformatie)* | **Noodzakelijk**<br>Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (MTD* 1 week)<br><br>*( bijv : primaire proces informatie)* |
| **Hoog / III**<br><br>**(zeer grote schade)** | **Geheim**<br>Informatie die alleen door medewerkers met een specifieke rol of functie mag worden ingezien, voor zover nodig voor hun taken en waartoe zij toegang hebben op basis van rol of functie<br>*( bijv : gezondheids-/medische en justitiële gegevens, informatie die beschermd moet worden tegen statelijke actoren)* | **Absoluut**<br>Onjuiste of onvolledige informatie kan grootschalige juridische consequenties hebben of leiden tot een crisissituatie met aanzienlijke financiële schade<br><br>*( bijv : specifieke gemeentelijke informatie op de website o.a. informatie waaraan rechten zijn te ontlenen, beschikkingen en besluiten)* | **Essentieel**<br>Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (MTD* 1 dag)<br><br>*( bijv : basisregistratie BRP, crisisbeheersing)* |