Werken in vertrouwen

Strategisch informatiebeveiligingsbeleid

Opdrachtgever	DT Kampen / MT Zwolle
Opdrachtnemer	Hetty van Hulsentop, Adri du Plessis, Marisa Götz, Allin Peter Britstra
Versie	1.0
Datum	21 november 2018

Datum 21 november 2018
Titel Werken in vertrouwen

Inhoud

1 Waarom informatiebeveiliging?

1.1 Inleiding

Voor u ligt het nieuwe Informatiebeveiligingsbeleid van Gemeente Kampen en Gemeente Zwolle. Deze vervangt het gezamenlijke Informatiebeveiligingsbeleid van beide gemeenten. Bij het evalueren van het oude beleid bemerkten we het praktische nut van gezamenlijk beleid. Hierom is besloten ook het nieuwe beleid gezamenlijk op te stellen. Hierom spreekt dit document in het vervolg over Gemeente Kampen/Zwolle, tenzij er een reden is om de gemeenten afzonderlijk te noemen.

Gemeente Kampen/Zwolle is een informatie-intensieve organisatie met een primaire focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente en hun ketenpartners moeten kunnen beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. Bovendien moeten burgers en bedrijven er op kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Hierom kent het informatiebeveiligingsbeleid van Gemeente Kampen/Zwolle vier pijlers:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid;
- controleerbaarheid.

Voor Gemeente Kampen/Zwolle is het belangrijk dat informatie **beschikbaar** is wanneer medewerkers en (keten)partners deze nodig hebben om hun taak uit te voeren. En dat burgers en bedrijven over informatie kunnen beschikken om diensten te verlenen of te benutten. Beschikbare informatie moet uiteraard wel **integer** zijn, dus juist en actueel. En **vertrouwelijke** informatie moet voldoende worden beschermd. Tenslotte moeten handelingen en besluiten aantoonbaar en daardoor **controleerbaar** zijn, zodat rapporteren en eventueel auditen mogelijk is.

Voorliggend document bevat de visie waarmee Gemeente Kampen/Zwolle haar informatiebeveiliging wil bouwen op bovengenoemde vier pijlers. Om dit te verwezenlijken wordt informatiebeveiliging vormgegeven door maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard. De daadwerkelijke aanpak staat niet in dit strategisch beleidsdocument, wel de organisatie van informatiebeveiliging en de verantwoording erover.

1.2 Vertrouwen op verantwoordelijkheid

Middels tactisch beleid werkt Gemeente Kampen/Zwolle de vier beschreven pijlers uit. Die uitwerking biedt handvatten aan medewerkers om het werk op een professionele manier uit te voeren. Dit vraagt naast het kunnen beschikken over de juiste middelen om een bewuste houding. Bewust van de kansen die digitaal werken biedt voor burgers en bedrijven. En bewust van de risico's ten aanzien van vertrouwelijke en persoonlijke

gegevens, waarmee die kansen worden gerealiseerd. En daarom bewust van de middelen die de organisatie aanbiedt om de kansen veilig te benutten.

Die bewuste houding ontstaat niet vanuit het niets. Medewerkers worden geïnformeerd over de aanwezigheid van ondersteunende middelen en hoe deze praktisch en veilig benut kunnen worden. En medewerkers worden geïnformeerd over de mogelijke bedreigingen waaraan onze informatiehuishouding tegenwoordig bloot staat. Waarbij uiteraard ook wordt geleerd hoe deze bedreigingen het hoofd te bieden.

Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis tot zich te nemen en toe te passen. En het is aan de leidinggevenden om deze professionele houding te ondersteunen en waar nodig te stimuleren. Daarbovenop is het aan de leidinggevenden om keuzes te maken, want alle risico's 100% afdichten is een utopie.

1.2.1 Veranderende omgeving

Informatisering en het integreren of koppelen van systemen speelt een steeds prominentere rol in de gemeentelijke organisatie. Hierdoor is Gemeente Kampen/Zwolle steeds afhankelijker van goed werkende informatievoorziening en -systemen. Dit betekent dat de gemeente alert is op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet van oorsprong zijn ontworpen met het oog op veiligheid. De veiligheid die met de technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en procedures. Daarnaast speelt echter de menselijke factor (het menselijk gedrag) een doorslaggevende rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk.

De veiligheid van informatie speelt binnen een groot aantal gebieden van de gemeente een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD) , de beveiligingsnorm DigiD of de Basisregistratie Adressen en Gebouwen (BAG) separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatieveiligheidsbeleid op te stellen voor alle organisatie onderdelen.

1.3 Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG;
- Archiefwet / Archiefregeling;
- Beveiligingsnorm DigiD

- Databankenwet;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie Grootschalige Topografie (BGT);
- Wet Basisregistratie Ondergrond (BRO);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet op de ruimtelijke ordening (Wro).

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

2 Visie op informatiebeveiliging

Informatie is één van de belangrijkste bedrijfsmiddelen van Gemeente Kampen/Zwolle. Zonder actuele en betrouwbare informatie, op de juiste plaats en op de juiste tijd, kunnen wij onze taken niet naar behoren vervullen. We werken met informatie om diensten te leveren aan onze inwoners en bedrijven, en om richting te geven aan de ontwikkeling van onze gemeente. We zijn open en transparant in wat we doen en waarom we het doen. We helpen onze inwoners en bedrijven 'in één keer goed' en voorkomen dat we dezelfde vraag twee keer stellen door goed gebruik van de informatie die wij hebben. Om dit te kunnen doen zien wij informatie als 'open tenzij'.

Maar met een nadrukkelijke 'tenzij', omdat informatie privacy of belangen van personen of organisaties kan schaden. Het is onze verantwoordelijkheid om deze rechten te beschermen. Zodat iedereen erop kan vertrouwen dat zorgvuldig met zijn/haar gegevens wordt omgegaan en dat privacy gewaarborgd is. Wij zoeken daarbij naar een goede balans tussen de te nemen maatregelen en het behouden van een goede en efficiënte dienstverlening, een transparant proces en acceptabele kosten. De uitgangspunten in dit informatiebeveiligingsbeleid zijn in lijn met het Privacyreglement 2018-2021 van Gemeente Kampen en de Regeling bescherming persoonsgegevens van Gemeente Zwolle.

Wij zorgen ervoor dat we bewust en veilig omgaan met informatie door een combinatie van organisatorisch en technische borgen van de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid en privacy en tijdige signalering en opvolging van incidenten. We zijn transparant: we maken inzichtelijk waarvoor wij de gegevens van onze inwoners gebruiken, en bieden mogelijkheden tot inzage in het eigen dossier of tot een verzoek voor wijziging/ vernietiging van de eigen gegevens.

Onze verantwoordelijkheid voor informatiebeveiliging en privacy beperkt zich niet tot onze eigen organisatie. Ook in samenwerking met andere organisaties nemen wij onze verantwoordelijkheid voor het zorgvuldig omgaan met informatie en privacy in de keten door te zorgen voor duidelijke afspraken over deze onderwerpen.

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging en privacy steeds belangrijker worden. Toenemende digitalisering en samenwerking met andere partijen in dienstverleningsketens leidt tot meer en makkelijker uitwisselen van informatie. Onze inwoners en bedrijven willen snel en digitaal geholpen worden, maar willen dit doen met behoud van hun recht op privacy. Onze medewerkers willen en moeten steeds meer 'anyplace en anytime' kunnen werken, maar dit mag niet leiden tot informatie die 'op straat ligt'. En onze kantooromgeving ontwikkelt zich, door 'het nieuwe werken' en samenwerking met andere partijen, tot een ontmoetingsplek waarin de gemeente gastheer is. Het beveiligen is daarbij extra lastig omdat een deel van onze kantooromgeving vrij toegankelijk moet blijven.

Daarom zetten we de komende jaren in op het optimaliseren van de informatieveiligheid en privacy en het verder professionaliseren van de informatiebeveiligingsfunctie. Zodat

we blijven aansluiten op de veranderende wetgeving op het gebied van persoonsgegevens, en informatiebeveiliging en privacy bij alle ontwikkelingen vanaf het begin als belangrijk thema worden meegenomen.

2.1 Tien richtinggevende principes

We zorgen ervoor dat we als Gemeente Kampen/Zwolle onze informatiebeveiliging (en als onlosmakelijk onderdeel daarvan de privacy) goed georganiseerd hebben en houden. Met als richtinggevende principes die gehanteerd moeten worden bij de invulling dat:

1. aan wetgeving voldaan moet worden, met als voorbeelden (niet uitputtend) de wetgeving op het gebied van de Basisregistratie Personen (BRP), Structuur Uitvoeringsorganisaties Werk en Inkomen (SUWI) of Archiefwet;
2. we de Baseline Informatiebeveiliging Overheid (BIO) en de onderliggende code voor informatiebeveiliging (NEN/ISO 27002) als basis voor de inrichting van onze informatiebeveiliging gebruiken;
3. we binnen deze kaders gaan voor het beheersen van risico's tegen acceptabele kosten, waarbij we een zorgvuldige en transparante afweging maken van informatiebeveiliging en het recht op privacy versus de gewenste transparantie en het 'in één keer goed' onze diensten kunnen leveren;
4. toegang tot, gebruik van en uitwisseling van vertrouwelijke / geheime informatie aantoonbaar gebonden moet zijn aan het vervullen van een aan onze gemeente toegewezen taak. Het is transparant voor de inwoner of er wel of niet toestemming gegeven moet worden voor gebruik of uitwisseling;
5. informatiebeveiliging niet alleen om techniek en procedures gaat maar vooral om mensen en gedrag, en dat daarom de verantwoordelijkheid voor informatiebeveiliging bij het lijnmanagement ligt, met het college van burgemeester en wethouders als eindverantwoordelijke;
6. dat we bij samenwerking in ketens, bij uitbesteed werk of in samenwerkingsverbanden verantwoordelijk blijven voor informatiebeveiliging. In de samenwerking met andere overheidsinstellingen gaan we uit van het 'Schengen principe' als zij aantoonbaar hun informatie conform wetgeving en richtlijnen beveiligen. Wij zijn transparant in welke informatie wij met hen uitwisselen en welke afspraken we gemaakt hebben;
7. het toepassen van het beleid, namelijk veilig omgaan met informatie, een zaak voor iedereen is die werkt namens de gemeente. Ongeacht of deze vast of tijdelijk in dienst is of iemand die bij een partner of ingehuurd werkzaamheden voor ons verricht;
8. elke medewerker weet wat informatiebeveiliging en privacy inhouden en zich ervan bewust is dat hij/zij een duidelijke eigen verantwoordelijkheid heeft. Zowel in het zelf veilig omgaan met en uitwisselen van informatie als in het melden van 'beveiligingsincidenten';
9. informatiebeveiliging om toezicht en onderhoud vraagt en een integraal onderdeel moet zijn in de (plan-do-check-act cyclus van de) bedrijfsvoering;
10. informatiebeveiliging onafhankelijke regie vraagt en af en toe ingrijpen in bestaande structuren, en dus centrale en onafhankelijke functionarissen.

2.2 De informatieveiligheidspiramide

Dit document is gebaseerd op de richtlijnen uit de strategische Baseline Informatiebeveiliging Nederlandse Gemeenten[1] (VNG/IBD). Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking worden gesteld, zoals de Wet basisregistratie personen (Wet BRP), Algemene verordening gegevensbescherming (AVG), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet openbaarheid bestuur (Wob).

Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet Basisregistratie Adressen en Gebouwen (Wet BAG), Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKBP), de Wet ruimtelijke ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

Teneinde de scope van dit document te verduidelijken, is in figuur 1 aangegeven welke niveaus van informatieveiligheid zijn te onderkennen.

Bovenaan de piramide treffen we het informatieveiligheidsbeleid aan. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen.

De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren Informatieveiligheidsanalyse. Tijdens deze Informatieveiligheidsanalyse wordt

- de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatieveiligheidsbeleid, en aan de beveiligingsmaatregelen uit de geldende baseline (zie H2.4). Dat gebeurt in samenwerking met de verantwoordelijken voor beveiligingsmaatregelen, die aangeven in hoeverre deze zijn geïmplementeerd. Onderdeel daarvan is ook een rondgang door het gebouw.
- een risico inventarisatie en evaluatie (RI&E) uitgevoerd waarin wordt ingeschat hoe kwetsbaar de gemeente is op basis van een risicocatalogus met informatieveiligheidsrisico's.

In de Informatieveiligheidsanalyse worden niet alleen de 'harde aspecten' onderzocht. Dat wil zeggen de techniek, de regels en de procedures, maar worden ook de 'zachte aspecten' meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie.

[1] Op het moment van schrijven is voor gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) van kracht. Per 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) van kracht. Veel handreikingen zijn nog gebaseerd op de BIG, uitgangspunt voor ons beleid is de BIO.

In de derde laag volgt, na de Informatieveiligheidsanalyse, de vorming van een actieplan. Tijdens deze stap worden de geconstateerde risico's gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van de risico's en de te treffen maatregelen.

- Het actieplan komt tot stand door middel van een prioriteringssessie waarin de gemeente Kampen/Zwolle zelf aangeeft welke specifieke verbeteracties zij willen en kunnen oppakken voor een periode van één tot twee jaar;
- Naast het formuleren van de specifieke verbeteracties worden onder andere de uitvoerders, de kosten en de planning vastgelegd;
- Dit compacte actieplan vormt de praktische leidraad voor de te implementeren maatregelen van de Baseline Informatiebeveiliging Overheid door de beveiligingsorganisatie onder verantwoordelijkheid van de Chief Information Security Officer (CISO, zie H3.3.1).

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals de BRP, de BAG of het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen zoals het gebruikersbeheer van Suwinet, de inrichting van de ICT-platformen of de juistheid van de uitkerings- of crediteurenadministratie.

Figuur 1: informatiebeveiligingspiramide (bron: BMC)

2.3 Risicobenadering

Het invoeren van maatregelen gebeurt vanuit een risicobenadering: de effecten van de maatregelen moeten in verhouding staan tot de noodzakelijke beveiliging. Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen gebruiken we beveiligingsclassificaties. Deze geven aan welk beschermingsniveau noodzakelijk is voor welke proces en/of informatiesysteem, en maakt duidelijk welke maatregelen genomen moeten worden. Het beschermingsniveau is gebaseerd op de classificatie van

data, waarvoor de Informatiebeveiligingsdienst van de VNG een handreiking biedt. In onderstaande tabel wordt de classificatie samengevat weergegeven.

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0	**Openbaar** informatie mag door iedereen worden ingezien *(bv. algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv. templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd (weken) niet beschikbaar zijn *(bv. ondersteunende tools als routeplanner)*
Laag / I	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv. informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv. rapportages)*	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn (bij calamiteiten maximaal enkele dagen) *(bv. administratieve gegevens)*
Midden / II	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv. persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv. bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (bij calamiteiten maximaal een dag) *(bv. voorwaardelijke primaire proces informatie)*
Hoog / III	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv. Bijzondere persoonsgegevens zoals zorggegevens, strafrechtelijke informatie en omvattende financiële informatie (SUWI))*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv. specifieke gemeentelijke informatie op de website o.a. waaraan rechten zijn te ontlenen)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (bij calamiteiten minder dan een dag) *(bv. basisregistraties BRP en SUWI)*

De proceseigenaar (vaak een afdelingshoofd) bepaalt welke maatregelen genomen moeten worden op basis van een risicoanalyse[2], waarbij de kans en het effect het risico bepalen. De door de proceseigenaar gemaakte risicoafweging, tussen enerzijds het risico en anderzijds de kosten en consequenties van de maatregelen conform de beschermingseisen, wordt vastgelegd evenals de te treffen maatregelen. Uit de kleuren in de tabel blijkt de impact van deze maatregelen, deze zijn nu nog afgeleid van de BIG. Zaken binnen de donkerblauw gearceerde vakken in de tabel worden afgedekt wanneer de BIG-beveiligingsmaatregelen zijn ingevoerd. Voor zaken in de lichtblauw gekleurde vlakken dienen (bovenop de BIG) aanvullende beveiligingsmaatregelen te worden getroffen.

Sturing op de implementatie van te treffen maatregelen is een doorgaand proces, waarin aandacht is voor continue verbetering. De hiervoor noodzakelijke PDCA (Plan-Do-Check-Act) cyclus – de kwaliteitscyclus – is onderdeel van ons Information Security Management System (ISMS, zie H3.2).

2.4 Gezamenlijke basis

De tactische implementatie van informatiebeveiliging binnen Gemeente Kampen/Zwolle is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), die naar verwachting 1 januari 2020 van kracht wordt en waarop gemeenten zich vanaf 2019 gaan voorbereiden. Deze baseline, afgeleid van de internationale ISO-standaard voor informatiebeveiliging, vervangt diverse afzonderlijke overheidsbaselines en is de gezamenlijke basis voor de gehele Nederlandse overheid. Want beveiligen van informatie kunnen we als gemeente niet alleen. In een netwerksamenleving, waarin systemen en organisaties steeds meer met elkaar verweven raken, zijn alle partners samen aan zet om de informatieveiligheid te borgen.

Een deel van de gegevens die medewerkers van Gemeente Kampen/Zwolle en onze partners gebruiken komt uit bronsystemen waarvoor bijzondere eisen gelden. Denk aan basisregistraties als de BRP en de BAG of Suwinet. Gemeente Kampen/Zwolle is zich bewust van de eisen die verbonden zijn aan het gebruik van (soms zeer gevoelige) gegevens uit deze bronnen. De voor deze toepassingen geldende richtlijnen en normenkaders vormen voor Gemeente Kampen/Zwolle de basis waarop deze binnen de organisatie mogen worden benut. In enkele gevallen zijn er specifieke functionarissen binnen de gemeente aangewezen om hierop toe te zien. Deze functies staan beschreven in het hoofdstuk “Organisatie van informatiebeveiliging”.

2.5 Gedeelde uitdaging

Inzet voor Gemeente Kampen/Zwolle is standaardisatie en samenwerking. Via de Informatiebeveiligingsdienst (IBD) van de VNG werken we aan gezamenlijke aanpak en

[2] Een risicoanalyse bestaat minimaal uit een Business Impact Analyse, waarin ook de risico’s omtrent persoonsgegevens aan de orde komen. Blijkt daaruit dat in een proces persoonsgegevens van belang zijn, dan zal ook een Privacy Impact Analyse deel moeten uitmaken van de risicoanalyse.

ondersteuning op landelijk niveau. Dit is zeker van belang als er een vuist gevormd moet worden richting bijvoorbeeld leveranciers.

Via het Shared Service Centrum ONS implementeren we gezamenlijk met Gemeente Zwolle/Kampen en Provincie Overijssel diverse IT-security maatregelen. Hoewel provincie en gemeentes andere organisaties zijn, dienen zij dezelfde burgers. Ook gaan beide overheidslagen vanaf 2019 de informatiebeveiliging op dezelfde basis funderen (BIO). Onze inzet zal daarom gericht zijn op steeds nauwere samenwerking met alle bij het SSC-ONS betrokken partners. Omdat we van mening zijn dat we samen sterker en efficiënter een veilige informatiehuishouding kunnen borgen.

2.5.1 GGI-Veilig

Via VNG Realisatie bouwen gemeenten aan de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI). GGI is een veilige, samenhangende digitale infrastructuur die samenwerken tussen gemeenten en andere overheden beter, veiliger en gemakkelijker maakt. Eén van de programma's binnen GGI is GGI-Veilig, bedoeld om het GGI-Netwerk en de eigen gemeentelijke infrastructuren veiliger te maken en de digitale weerbaarheid van gemeenten te verhogen.

Met GGI-Veilig wordt een producten- en dienstenportfolio samengesteld en aanbesteed voor de inrichting, uitvoering en borging van het informatiebeveiligingsproces. Gemeenten Kampen en Zwolle omarmen deze samenwerking en hebben samen met Provincie Overijssel het mandaat verstrekt aan het SSC-ONS om namens de partners producten vanuit GGI-Veilig af te nemen en in te zetten.

3 Organisatie van de informatieveiligheid

3.1 Verantwoordelijkheid

Het college van Gemeente Kampen/Zwolle stelt middels het informatiebeveiligingsbeleid de kaders voor de organisatie en geeft hiermee richting aan de uitvoering van taken. De directie van Gemeente Kampen/Zwolle stuurt de organisatie in de door het college aangegeven richting.

Afdelingshoofden zijn als eigenaar verantwoordelijk voor de praktische uitvoering ervan binnen hun processen en systemen. Leidend hierbij zijn de maatregelen uit de BIO, in specifieke gevallen aangevuld met richtlijnen vanwege Suwinet, DigiD, PNIK, BRP of andere basisregistraties. Bij het vervullen van deze rol ontvangen zij richtlijnen en ondersteuning van de CISO en de adviseurs informatiebeveiliging. In een aantal gevallen benoemd de organisatie specifieke functionarissen ter ondersteuning van de uitvoering van informatiebeveiliging. Denk bijvoorbeeld aan de Security Officer Suwinet.

Orgaan	Verantwoordelijkheid
Gemeenteraad	Adviserend richting College en ‘horizontaal toezicht’
College van B&W	Eindverantwoordelijk (portefeuille P&O), stelt het strategisch informatieveiligheidsbeleid vast en rapporteert jaarlijks aan de Raad in het jaarverslag.
Gemeentesecretaris/ directie	Ambtelijk eindverantwoordelijk en stelt het tactisch informatieveiligheidsbeleid vast.
Chief Information Security Officer	Stelt informatiebeleid op en coördineert de uitvoering ervan, beheerst risico’s en rapporteert aan management en College.
Afdelingshoofden/ proceseigenaren	Informatieveiligheid eigen processen, risico-afweging, implementatie, toezicht en sturing op naleving eigen proces.
Medewerkers	Medewerkers zijn verantwoordelijk voor de uitvoering.

3.2 Verantwoording

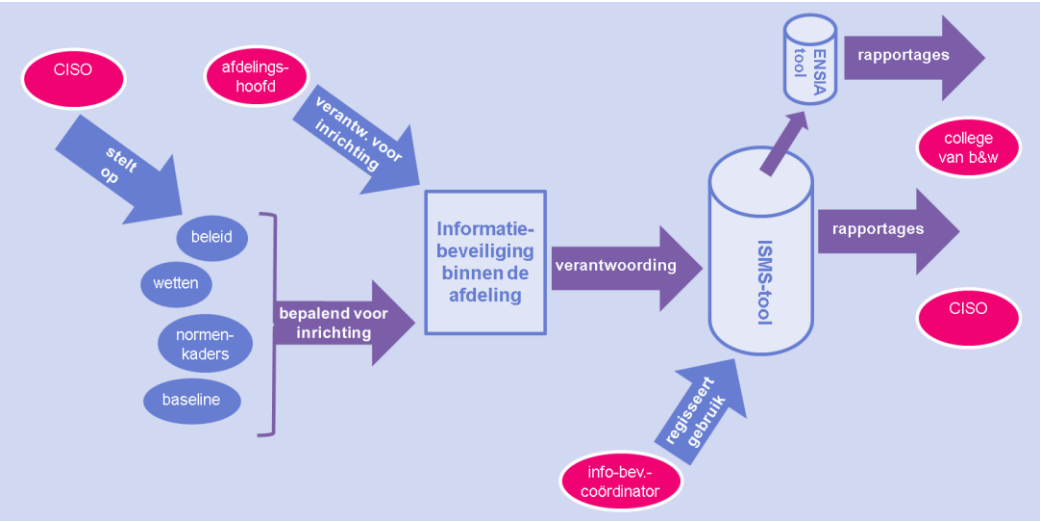
Afdelingshoofden leggen verantwoording af over de wijze waarop zij informatiebeveiliging borgen. Gemeente Kampen/Zwolle zet een ISMS-tool in om hen hierbij te ondersteunen. ISMS staat voor Information Security Management System en is het geheel van maatregelen en processen dat de informatiebeveiliging borgt, anders gezegd: het ‘kwaliteitssysteem informatiebeveiliging’. In de ISMS-tool worden maatregelen en taken toegewezen aan functionarissen, die daar vervolgens het resultaat en bijbehorende bewijslast aan koppelen.

Vanuit de ISMS-tool kan gerapporteerd worden over de stand van de informatiebeveiliging binnen Gemeente Kampen/Zwolle. Ieder kwartaal ontvangt de CISO een overzicht van de status. Dit voedt, samen met een rapportage vanuit de incidentenregistratie en input vanuit de gemeentelijke organisatie en externe bronnen,

het kwartaalverslag van de CISO over de stand van de informatiebeveiliging. Dit verslag wordt door de CISO verstrekt aan de directie en het college van Gemeente Kampen/Zwolle.

Op basis van de kwartaalrapportages en een jaaroverzicht vanuit de ISMS-tool legt het college van Gemeente Kampen/Zwolle jaarlijks verantwoording af over de stand van de informatiebeveiliging. De formele verantwoording verloopt via de ENSIA-systematiek, de Eenduidige Normatiek Single Information Audit. Vanuit de gemeentelijke ISMS-tool wordt hiervoor de door het rijk ingerichte ENSIA-tool gevuld.

ENSIA biedt handvatten om de verantwoording te stoelen op de geldende baseline. Deze verantwoording zal de komende jaren steeds nauwer aansluiten op de gemeentelijke P&C-cyclus. Zo krijgt het gemeentebestuur overzicht over de stand van de informatiebeveiliging en kan zij hier beter op sturen. Via de ENSIA-systematiek wordt ook verantwoording afgelegd aan diverse externe toezichthouders op enkele specifieke aandachtsgebieden, zoals Suwinet, BRP, PNIK en DigiD.



Figuur 2: het kwaliteitssysteem informatiebeveiliging (ISMS)

3.3 Informatieveiligheidsorganisatie

3.3.1 Functionarissen en hun rol ten aanzien van informatiebeveiliging

CISO

De Chief Information Security Officer (CISO) is op organisatieniveau verantwoordelijk voor het actueel houden van informatiebeveiligingsbeleid, het coördineren van de uitvoering van beleid, het beheersen van risico's en het opstellen van rapportages.

Adviseur informatiebeveiliging

De adviseur informatiebeveiliging is op organisatieniveau verantwoordelijk voor het opstellen van informatiebeveiligingsbeleid, het stimuleren van bewust omgaan met informatie binnen de organisatie, het ondersteunen van risicoanalyses en het adviseren van projecten.

Coördinator informatiebeveiliging
De coördinator informatiebeveiliging is op organisatieniveau verantwoordelijk voor het toezicht op de naleving van het informatiebeveiligingsbeleid, de realisatie van beveiligingsmaatregelen, het ondersteunen van rapportages (waaronder ENSIA) en het escaleren van beveiligingsincidenten.

Afdelingshoofden
De afdelingshoofden zijn als eigenaar integraal verantwoordelijk voor de (informatie)beveiliging van de processen en systemen binnen hun afdeling. Daaronder valt in ieder geval:

- het classificeren van opgeslagen data in applicaties en gegevensverzamelingen;
- medewerkers attenderen op hun verantwoordelijkheid voor informatiebeveiliging in hun dagelijkse taken;
- het laten uitvoeren van een informatiebeveiligingsanalyse op de processen en (informatie)systemen van de afdeling;
- het kiezen, (laten) uitvoeren en uitdragen van maatregelen die voor de afdeling van toepassing zijn, op basis van de informatiebeveiligingsanalyse;
- het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- het rapporteren, via de coördinator informatiebeveiliging, over het voldoen aan wet en regelgeving en organisatiebeleid (compliance) in de P&C rapportages.

Medewerkers
Alle medewerkers zijn verantwoordelijk voor het veilig uitvoeren van hun eigen functie en taken. Zij gaan zorgvuldig en gedisciplineerd om met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen die voor hun werkproces gelden vanwege beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

3.3.2 Functionarissen met een specifieke beveiligingsfunctie

Beveiligingsbeheerder BRP
De beveiligingsbeheerder BRP is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid voor de gemeentelijke voorziening van de BRP. Deze functie is vastgelegd en beschreven in de Beheerregeling Gemeentelijke Basisregistratie Personen van Gemeente Kampen en in de Regeling beheer en toezicht Basisregistratie Personen van Gemeente Zwolle.

Privacybeheerder BRP
De privacybeheerder adviseert de informatiebeheerder BRP over de privacyaspecten die voortvloeien uit de uitvoering van de Wet en Verordening BRP. Deze functie is vastgelegd en beschreven in de Regeling beheer en toezicht Basisregistratie Personen van Gemeente Zwolle en de Beheerregeling Gemeentelijke Basisregistratie Personen van Gemeente Kampen.

Beveiligingsfunctionaris reisdocumenten

Datum 21 november 2018
Titel Werken in vertrouwen

De beveiligingsfunctionaris reisdocumenten is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures reisdocumenten en rijbewijzen.

Security Officer Suwinet
De Security Officer Suwinet bevordert en bewaakt, in opdracht van de interne eigenaar, het veilig gebruiken van Suwinet door medewerkers (in- en extern) van de gemeente Zwolle.

Beheerders van basisregistraties
Voor elke basisregistratie waarvan Gemeente Kampen/Zwolle bronhouder is, draagt een beheerder de verantwoordelijkheid voor het inwinnen en bijhouden van de authentieke en niet-authentieke gegevens in een basisregistratie en voor het borgen van de kwaliteit van die gegevens.

3.3.3 Functionarissen met een specifieke privacy functie

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming is de interne toezichthouder op de verwerking van persoonsgegevens binnen Gemeente Kampen/Zwolle. Deze functionaris dient binnen Gemeente Kampen/Zwolle aanwezig te zijn volgens artikel 37 van de Europese Algemene Verordening Gegevensbescherming (AVG). Taken en verantwoordelijkheden van de Functionaris Gegevensbescherming staan, conform artikel 39 van de AVG, beschreven in het Privacyreglement 2018-2021 van Gemeente Kampen en de Regeling bescherming persoonsgegevens van Gemeente Zwolle.

Privacy Officer
De Privacy Officer ondersteunt de Functionaris Gegevensbescherming bij het uitoefenen van toezicht binnen Gemeente Kampen/Zwolle. Daarnaast traint de Privacy Officer het lijnmanagement en medewerkers in het zorgvuldig omgaan met persoonsgegevens en ondersteunt hen bij vragen over privacy en persoonsgegevens.

3.3.4 Overleg en afstemming met SSC ONS en deelnemende partners

BTO Security Board
Doel:
- voortgang en afstemming IT-security zaken binnen het SSC-ONS in relatie tot ontwikkelingen bij de deelnemende partners;
- planning en voortgang van projecten en audits;
- voorbereiden SPO agendapunten m.b.t. informatiebeveiliging.

Frequentie is maandelijks.
Deelnemers zijn de Chief Information Security Officer (voorzitter) en de Technical Information Security Officer van het SSC-ONS, en informatiebeveiligingsvertegenwoordigers van de partners.

3.3.5 Overleg en afstemming binnen Gemeente Kampen

Overleg Privacy en Informatiebeveiliging
Doel:
- Voortgang en afstemming inzake privacy en informatiebeveiligingszaken
- Voorbereiden beleidsstukken

Frequentie is tweewekelijks
Deelnemers zijn FG, Privacy Officer en CISO/coördinator informatiebeveiliging

Platform Informatieveiligheid (PIV)
Doel:
- gemeentebrede afstemming over informatiebeveiligingszaken en ENSIA

Frequentie is minimaal vier keer per jaar.
Deelname door ambassadeurs voor het thema informatiebeveiliging vanuit:
- CISO/Coördinator informatiebeveiliging, voorzitter
- ICT Beheer (SSC ONS)
- Personeelszaken
- Facilitaire zaken
- BRP (Burgerzaken)
- Beheer basisregistraties
- DigiD beheer
- Suwi-beheerder/Sociaal domein
- DIV beheerder
- FG en Privacy Officer
- Controller en interne controle

Beveiligingsoverleg Suwinet
Doel:
- Voortgang en afstemming inzake informatiebeveiligingszaken m.b.t. het gebruik van Suwinet.

Frequentie is maandelijks.
Deelnemers zijn teammanager Backoffice MO, security officer MO, functioneel beheerder MO en CISO/coördinator informatiebeveiliging.

3.3.6 Overleg en afstemming binnen Gemeente Zwolle

Overleg Privacy en Informatiebeveiliging
Doel:
- Voortgang en afstemming interne P&IB-zaken
- Voorbereiden beleidsstukken

Frequentie is minimaal driewekelijks.
Deelnemers zijn de CISO (voorzitter), FG, Privacy Officer en de adviseur(s) informatiebeveiliging.

Werkgroep Informatiebeveiliging
Doel:
- gemeentebrede afstemming van activiteiten en beleid t.a.v. informatiebeveiliging.

Frequentie: minimaal vier keer per jaar.
Deelname door ambassadeurs voor het thema informatiebeveiliging vanuit:
- Burgerzaken
- CISO, voorzitter
- Informatievoorziening (Dataprotectie; Functioneel beheer; Gegevensmanagement; Informatieveiligheid)
- HR
- Interne Controle

Datum 21 november 2018
Titel Werken in vertrouwen

- Privacy
- Services
- Suwinet
- Website (Team Digitale Regie)

Bijlage 1: begrippenlijst

Begrip	Uitleg
Audit	Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid.
Autoriseren	Het toekennen van rechten aan (groepen van) personen, processen en/of systemen.
Beschikbaarheid	Beschikbaarheid geeft aan in hoeverre informatie (bijvoorbeeld via een ICT-dienst, systeem of een document) toegankelijk is voor de geautoriseerde gebruikers.
CISO	De CISO (Chief Information Security Officer) bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert over de stand van zaken.
Classificatie	Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.
Controleerbaarheid	De mate waarin de juistheid en volledigheid van de informatie kunnen worden gecontroleerd.
Dataclassificatie	Classificatie (of rubricering) van data geeft antwoord over de hoeveelheid maatregelen die genomen moeten worden om die data adequaat te beschermen.
ENSIA	ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.
Functiescheiding	Het scheiden van gerelateerde taken en bevoegdheden om fouten en fraude te voorkomen.
Functionaris Gegevensbescherming	De functionaris voor de gegevensbescherming (FG) houdt binnen een organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
IBD	De Informatiebeveiligingsdienst voor gemeenten (IBD) werkt aan het verhogen en op peil houden van de informatiebeveiliging van Nederlandse gemeenten vanuit de kracht van het collectief. De IBD is een initiatief van alle Nederlandse gemeenten. Alle gemeenten, intergemeentelijke sociale diensten en belastingsamenwerkingen kunnen gebruik maken van de diensten van de IBD.
Informatie	Een verzameling van gegevens (met of zonder context) opgeslagen in gedachten, geschriften en/of digitale informatiedragers.

Begrip	Uitleg
Integriteit	Een kwaliteitskenmerk voor gegevens, een object of een dienst, dat aangeeft dat het gegeven juist (rechtmatig), volledig (niet te veel, niet te weinig), tijdig en geautoriseerd (gemuteerd door wie dat mag) is.
Persoonsgegeven	Ieder gegeven dat is te herleiden tot een individuele persoon, zoals naam, adres, geboortedatum, maar ook kenteken en telefoonnummer.
Privacy	Privacy is de persoonlijke levenssfeer die onszelf en ons handelen, eigenschappen en informatie onderscheidt en afschermt van anderen.
Privacy officer	Ondersteunt en adviseert bij alle gemeentebrede privacyvraagstukken.
Reisdocument	Een reisdocument is een document dat de houder toestemming verleent tot het betreden van en reizen door een bepaald land of gebied. Nederland kent de volgende soorten reisdocumenten: nationaal paspoort; zakenpaspoort; 2e paspoort; diplomatiek paspoort; dienstpaspoort; reisdocument voor vreemdelingen; reisdocument voor vluchtelingen; noodpaspoort; laissez-passer[3].
Schengen principe	Met het Schengen principe wordt bedoeld dat organisatie-onderdelen van de overheid elkaar beschouwen als vertrouwd partner en niet als onvertrouwde buitenwereld. Het gevolg hiervan is dat iedere overheidsorganisatie afzonderlijk zijn omgeving beveiligt en 'schoon' houdt en dat de andere omgevingen hierop kunnen vertrouwen.
Vertrouwelijkheid	Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gemachtigd is het gegeven te benaderen.

[3] Bron: https://www.rijksoverheid.nl/onderwerpen/paspoort-en-identiteitskaart/vraag-en-antwoord/welke-soorten-reisdocumenten-zijn-er