GEMEENTE DOESBURG

Informatieveiligheidsbeleid gemeente Doesburg

Privacy- en Informatiebeveiligingsbeleid

2020 - 2022

Datum: januari 2020

Team: I&A

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	18 november 2019	A. Nas J. Versteegh	Definitief sjabloon opgesteld n.a.v. feedback samenwerking
1.01	21november 2019	Peter Stuart	Sjabloon ingevuld voor situatie gemeente Doesburg
1.02	26 november 2019	Peter Stuart	Opmerkingen van Jessica Tonneyck verwerkt
1.03	27 november 2019	Peter Stuart	Onderdeel controle en verantwoording afgestemd met Hans Visser
1.04	22 januari 2020	Peter Stuart	Verwijzing naar beveiligingsrichtlijn SUWI gemeente Doesburg
1.05	27 mei 2020	Peter Stuart	Inleiding aangepast

Samenvatting

De gemeente Doesburg verwerkt, net als alle andere gemeenten, veel gegevens om haar taken goed uit te voeren. Burgers, bedrijven, ketenpartners en onze eigen medewerkers moeten erop kunnen vertrouwen dat informatie die wij verwerken betrouwbaar is én dat wij zorgvuldig omgaan met gegevens. Hiervoor is inzet van ons allemaal nodig.

Om veilig met informatie om te gaan is aandacht nodig voor de beveiliging van informatie (**informatiebeveiliging**) én de bescherming van persoonsgegevens (**privacy**). Met één woord noemen we dit '**Informatieveiligheid**'.

Om de veiligheid van de informatie te waarborgen en de risico's goed in beeld te hebben is dit beleid opgesteld. Dit beleid is gebaseerd op het normenkader zoals beschreven in de **Baseline Informatiebeveiliging Overheid (BIO)** en de **Algemene Verordening Gegevensbescherming (AVG)**.

In hoofdstuk 2.4.2 van dit beleid zijn de belangrijkste uitgangspunten verwoord. Zoals het inrichten en verankeren van informatieveiligheid in de organisatie waarbij iedereen zijn of haar rol kent (zie hoofdstuk 3) en hierna kan handelen. Zo wordt informatieveiligheid een pijler waarop de organisatie is gebouwd.

De uitgangspunten zijn verdeeld in de categorieën **Mens, Organisatie** en **Techniek**. Er is gekozen voor deze driedeling omdat informatieveiligheid meer is dan alleen het nemen van technische maatregelen (ICT). Door informatieveiligheid te benaderen vanuit de driedeling mens, organisatie en techniek ontstaat een adequate bescherming van informatie.

Om uitvoering te geven aan dit beleid worden de uitgangspunten verder uitgewerkt, zie hiervoor bijlage 1. Daarnaast zijn er procedures en werkinstructies voor aanvullende specifieke onderwerpen opgesteld. Denk bijvoorbeeld aan de BRP of de BAG. Hiervoor gebruiken wij de standaarden van onder andere VNG Realisatie en de Informatiebeveiligingsdienst (IBD).

Om te weten of we dit onderwerp goed oppakken leggen we jaarlijks verantwoording af via de **verplichte ENSIA audit** en de **AVG toetsing**. Daarnaast komt informatieveiligheid ter sprake in de P&C-gesprekken.

Met dit beleid willen we een vervolgstap zetten om de veiligheid van informatie en de bescherming van persoonsgegevens op het huidige niveau te behouden en vanuit dit punt verder te ontwikkelen. Om dit te realiseren hebben we iedereen nodig: **informatieveiligheid is van ons allemaal!**

Inhoud

1. Inleiding

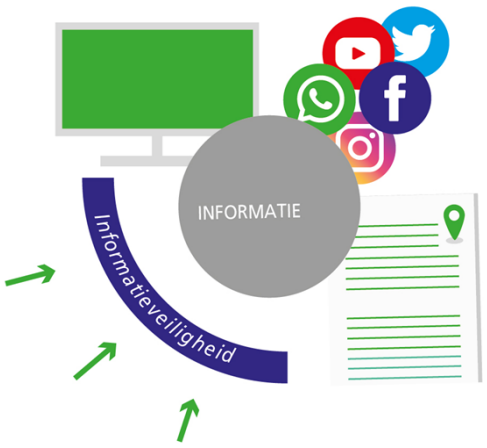
De gemeente Doesburg heeft een maatschappelijke verantwoordelijkheid: burgers, bedrijven, ketenpartners en onze eigen medewerkers moeten erop kunnen vertrouwen dat informatie die onze gemeente verwerkt betrouwbaar is en dat wij zorgvuldig omgaan met gegevens. Voor de uitvoering van haar taken is de gemeente steeds meer afhankelijk van informatiesystemen en informatiestromen. De veiligheid van informatie en het beschermen van gegevens neemt dan ook een belangrijke plek in.

Door de toenemende digitalisering verandert het werk bij de gemeenten. Er vindt een verschuiving plaats van handmatig uitgevoerde werkzaamheden naar steeds meer automatisering en digitalisering van de werkprocessen. Dit vereist ook andere competenties en vaardigheden van medewerkers. Een functie als Functioneel beheerder / applicatiebeheerder wordt hierin steeds belangrijker. Deze functies borgen dat de juiste mensen toegang hebben tot voor hen relevante Informatie en systemen en dat de systemen goed werken. Ook spelen ze een belangrijke rol bij het borgen van de informatieveiligheid.

Als de veiligheid van informatie onvoldoende is gewaarborgd, kunnen er risico's ontstaan. Risico's bij de uitvoering van gemeentelijke taken en het functioneren van de organisatie. Bovendien kunnen inbreuken op informatieveiligheid leiden tot financiële- en imagoschade. Kortom: informatieveiligheid is belangrijk en is van ons allemaal.

1.1 Wat is informatieveiligheid?

Informatieveiligheid gaat om het beschermen, beheren en beheersen van alle informatie. Je kan daarbij denken aan een digitale dreiging zoals diefstal van een wachtwoord. Maar ook analoge informatie op papier die alleen door de verkeerde persoon wordt ingezien. Door de toenemende digitalisering van de maatschappij neemt het risico op een inbreuk toe. Een goede inrichting van informatieveiligheid voorkomt schade die van invloed is op de kwaliteit van het functioneren van de gemeente.



Figuur 1: Wat is informatieveiligheid

1.1.1 Relatie tussen informatiebeveiliging en privacy

Informatieveiligheid valt uiteen in informatiebeveiliging en privacy. Zowel informatiebeveiliging als privacy gaat over het beschermen, beheren en beheersen van informatie. Waarbij privacy

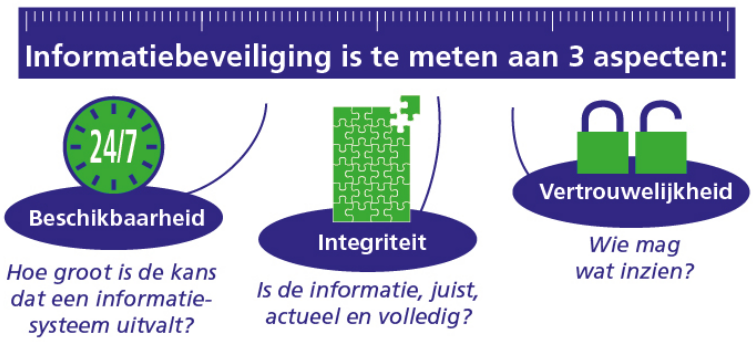
specifiek aandacht vraagt voor de bescherming van persoonsgegevens. Bij informatiebeveiliging gaat het juist om de bescherming van álle relevante organisatiegegevens. De onderwerpen zijn nauw met elkaar verbonden. In figuur 2 is de relatie tussen deze onderwerpen weergegeven.

Om veilig met informatie om te gaan is dus aandacht nodig voor de beveiliging van informatie én de bescherming van persoonsgegevens.

Figuur 2 – Verbondenheid privacy en informatiebeveiliging

1.1.2 Informatiebeveiliging

Bij informatiebeveiliging is de betrouwbaarheid van informatie belangrijk omdat je zorgvuldig met gegevens wilt omgaan. Dit doen we door de risico's te bepalen op basis van de drie Basis Beveiligingsniveaus (BBN1, BBN2 en BBN3). Het BBN wordt bepaald met behulp van drie aspecten. Dit zijn de mate van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Het BBN niveau wordt voornamelijk bepaald door de vertrouwelijkheid. Als de vertrouwelijkheid op BBN2 uitkomt en de beschikbaarheid en/of de Integriteit op Hoog uitkomen dan is het eindresultaat BBN2 met als advies om voor Beschikbaarheid en/of integriteit een aanvullende risicoanalyse te doen. Aan de hand van deze drie aspecten wordt bepaald welke maatregelen nodig zijn in verhouding tot de grootte van het risico. De omvang van het risico is bepalend voor de te nemen maatregelen



Figuur 3: BIV aspecten

1.1.3 Privacy

Bij privacy gaat het om de bescherming van persoonsgegevens. Persoonsgegevens zijn alle gegevens waarmee je uit kunt komen bij een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens van burgers worden voornamelijk verzameld voor het goed uitvoeren van de onze wettelijke taken. De burger moet er daarom op kunnen vertrouwen dat de wij zorgvuldig en veilig met persoonsgegevens omgaat. Iedereen heeft recht op bescherming van zijn of haar persoonlijke levenssfeer.

1.2 Beleid

Dit beleid beschrijft de informatieveiligheid in de gemeente Doesburg voor de jaren 2020 tot en met 2022. Het beleid vervangt het huidige, in januari 2017 vastgestelde beleid: 'Gemeente breed Informatiebeveiligingsbeleid gemeente Doesburg'

Beschikbaarheid, integriteit en vertrouwelijkheid van informatie is een voorwaarde voor een rechtmatige, doelmatige en doeltreffende gemeente. Om hieraan te voldoen is dit richtinggevende en kader stellende informatieveiligheidsbeleid opgesteld. Dit beleid wordt verder aangevuld met onderwerp specifieke (schriftelijk) beleidsdocumenten, procedures en werkinstructies die afzonderlijk worden vastgesteld. Zie hiervoor hoofdstuk 4 van dit beleid. Per kalenderjaar wordt een informatieveiligheidsplan opgesteld waarin dit beleid is uitgewerkt in concrete maatregelen.

Met dit beleid zet de gemeente Doesburg een volgende stap om de veiligheid van informatie en de bescherming van gegevens op het huidige niveau te behouden en vanuit dit punt verder te ontwikkelen. Naast de uitgangspunten van AVG is ook de opzet van de BIO verwerkt in dit beleidsstuk. Na vaststellening van dit beleid zal er een GAP analyse plaatsvinden die input zal opleveren voor het eerste Informatieveiligheidsplan.

1.3 Samenwerkingen

1.3.1 Regionale samenwerking

Binnen de Achterhoek werken de gemeenten Aalten, Bronckhorst, Doesburg, Doetinchem, Oude-IJsselstreek en partijen Buurtplein, BUHA, Erfgoedcentrum Achterhoek en Liemers, Gruitpoort, Laborijn, Omgevingsdienst Achterhoek, Regio Achterhoek, Sportservice Doetinchem en Zwembad Rozengaarde samen. Zij maken gebruik van de ICT infrastructuur volgens het gastheerschapmodel met gemeente Doetinchem als gastheer. Het gastheerschapmodel is vastgelegd op basis van een convenant en een dienstverleningsovereenkomst (DVO) tussen gemeente Doetinchem en de deelnemers.

Op strategisch niveau van de ICT-A-samenwerking nemen de gemeentesecretarissen samen met de voorzitter ICT Boardroom, Teamleider ICT, Adviseur ICT de beslissingen. Besluitvorming

vindt in de ICT samenwerking plaats op basis van consensus waarbij de meerderheid beslist en de minderheid het besluit accepteert.

Op het gebied van informatieveiligheid heeft de samenwerking de volgende relevante overlegstructuren.

Naam overleg en invulling	Omschrijving
ICT-Automatiseringsoverleg *(Maandelijks overleg)*	Besluitvorming op tactisch niveau over ontwikkelingen in de ICT samenwerking door de ICT-A coördinatoren van de gemeenten. Voor Doesburg neemt de Adviseur Automatisering deel aan dit overleg.
Informatiseringsoverleg (Maandelijks overleg)	Overleg over updates en nieuwe ontwikkelingen in de Informatievoorziening die samen kunnen worden verkend en opgepakt. Voor Doesburg neemt de Adviseur Informatievoorziening deel aan dit overleg.
Privacy overleg (Maandelijks overleg)	In dit overleg worden privacy onderwerpen besproken, afgestemd en uitgewerkt. Voor Doesburg neemt de Privacy coördinator deel aan dit overleg.
Informatiebeveiliging overleg (Zes-wekelijks overleg)	In dit overleg worden informatiebeveiliging onderwerpen besproken, afgestemd en uitgewerkt. Voor Doesburg neemt de coördinator Informatiebeveiliging deel aan dit overleg.

1.3.2 Landelijke samenwerking

Vereniging Nederlandse Gemeenten (VNG) Realisatie
VNG Realisatie werkt samen met gemeenten aan oplossingen om de gemeentelijke uitvoering te verbeteren. Dit gebeurt op basis van het door gemeenten vastgelegde meerjarenplan Gezamenlijke Gemeentelijke Uitvoering (GGU) 2020-2024.

Informatiebeveiligingsdienst (IBD)
De IBD is de sectorale CERT (Computer Emergency Response Team) voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. En de IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers.

Nationaal Cyber Security Centrum (NCSC)
Het NCSC is onderdeel van het ministerie van Justitie en Veiligheid. De taken van het NCSC zijn geregeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Het NCSC informeert, analyseert, onderzoekt en adviseert op landelijke niveau over het onderwerp cybersecurity. En

heeft als doel om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en daarmee maatschappelijke ontwrichting te voorkomen.

Centrum Informatiebeveiliging en Privacybescherming (CIP)
Het CIP is een publiek-private netwerkorganisatie die bestaat uit overheidsbedrijven en marktpartijen die met een convenant verbonden zijn en een hoeveelheid uren hebben toegezegd in de samenwerking. Als samenwerkingsverband dragen ze bij aan informatieveiligheid van de Nederlandse overheid en de ketens waarin de organisaties samenwerken.

1.4 Ambitie en visie op het gebied van informatieveiligheid

In het collegeprogramma van de gemeente Doesburg staat dat wij er voor gaan zorgen dat de privacy en informatieveiligheid van en voor onze inwoners goed zijn geborgd.

We actualiseren tijdig ons Informatiebeveiligingsbeleid van de gemeente. We voeren praktische maatregelen door om het beveiligingsniveau te verhogen en we monitoren en evalueren regelmatig in samenspraak met de functionaris gegevensbescherming. We zorgen ervoor dat onze informatiebeveiliging op orde is en voldoet aan de landelijke normen (de BIO / ENSIA). Ook zorgen we dat de privacy goed geborgd is conform de AVG.

2. Strategisch beleid

2.1 Doelen

De doelen van het informatieveiligheidsbeleid zijn:

- Het beschermen en op behoorlijke en zorgvuldige wijze omgaan met informatie zodat de beschikbaarheid, integriteit, vertrouwelijkheid behouden blijft;
- Het waarborgen van de bescherming van persoonsgegevens (privacy);
- Het minimaliseren van informatieveiligheidsrisico's tot een acceptabel niveau.

2.2 Wetgeving en standaarden

Dit beleid is opgesteld op basis van wet- en regelgeving en verplicht gestelde normenkaders. De belangrijkste standaarden zijn de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG).

2.2.1 Informatiebeveiliging

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging voor de gehele overheid. Dit normenkader is gebaseerd op de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. De BIO bestaat uit 'controls' met bijbehorende 'maatregelen' en is gebaseerd op risicomanagement. De 'controls' zijn techniek- en organisatieonafhankelijk geschreven op het niveau waarop een auditor beoordeelt. Ze hebben een relatie met één of meer risico's en hebben tot doel bij te dragen aan de betrouwbaarheidseisen zoals die door de organisatie zijn gesteld.

2.2.2 Privacy

Voor de bescherming van persoonsgegevens volgen wij de wetgeving. De bescherming van de privacy is geregeld in de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), de Aanpassingswet AVG (AAVG) en daaraan gerelateerde regelgeving.

2.3 Scope

De scope van dit beleid omvat:

- alle Doesburgse gemeentelijke processen,
- alle onderliggende informatiesystemen,
- alle informatie-uitwisseling tussen de gemeente Doesburg en externe partijen (bijvoorbeeld woningbouwvereniging),
- het gebruik van informatie door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit beleid geldt ook voor onderstaande vakgebieden. Aanvullend op dit beleid hebben deze onderstaande vakgebieden specifieke beveiligingseisen. Deze worden in aparte documenten beschreven, zie hiervoor ook hoofdstuk 4.

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Paspoorten en Nederlandse identiteitskaarten (PNIK)
- Digitale persoonsidentificatie (DigiD)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)

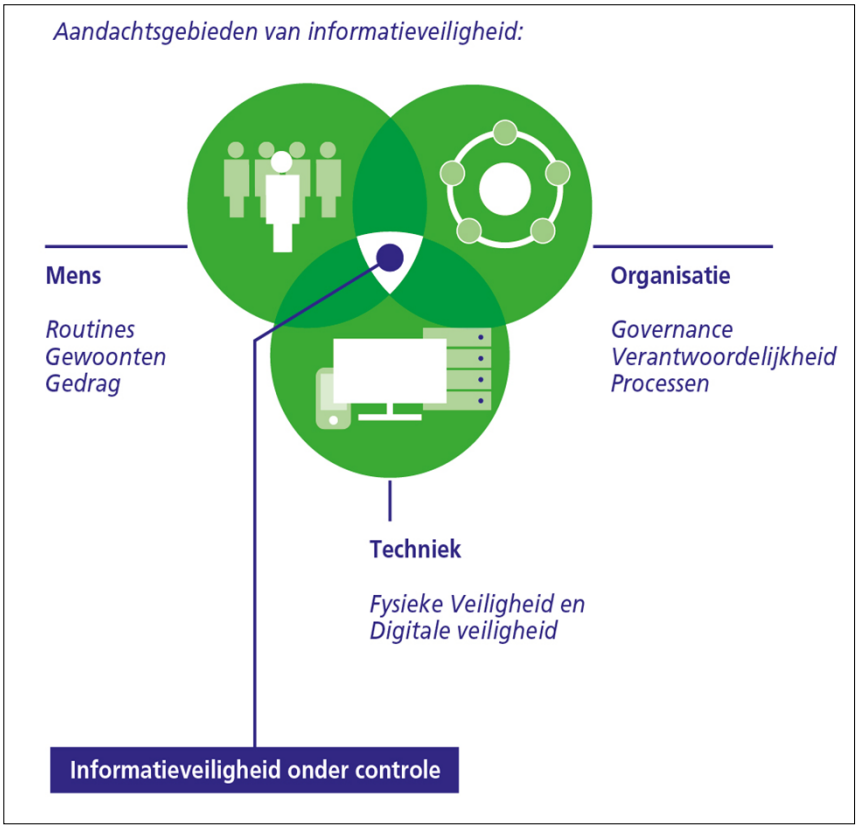
2.4 Uitgangspunten

Het college van B&W, de gemeentesecretaris en de teamleiders spelen een onmisbare rol bij het uitdragen en uitvoeren van dit beleid. Het management is verantwoordelijk voor het vaststellen van het belang dat informatie voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Dit beleid is van toepassing op de hele Doesburgse organisatie. Het is een kapstok voor verschillende procedures zoals weergegeven in hoofdstuk 4. De procedures worden periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.

2.4.1 Mens, Organisatie en Techniek

Bij informatieveiligheid gaat het om de bescherming van informatie in de breedste zin van het woord.



Figuur 4 – Mens, Organisatie en Techniek

Informatieveiligheid is meer dan alleen technische maatregelen (ICT). Door informatieveiligheid te benaderen vanuit de brede zin, via de aandachtsgebieden mens, organisatie en techniek, ontstaat een adequate bescherming van informatie.

2.4.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van dit beleid zijn:

Mens

- Iedere (vaste, tijdelijke, interne en externe) medewerker en bestuurder draagt bij aan het vergroten van bewustwording op het gebied van informatieveiligheid.
- Iedere medewerker en bestuurder is verplicht waar nodig gegevens te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- Iedere medewerker en bestuurder meldt een veiligheidsincident.

Organisatie

- Het college van B&W is eindverantwoordelijk voor:
    - Een actueel informatieveiligheidsbeleid en stelt de benodigde mensen en middelen beschikbaar om dit beleid vast te stellen en uit te voeren.
    - Het inrichten en implementeren van een informatieveiligheidsorganisatie met een Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG), informatieveiligheidscoördinatoren en -beheerders.
    - Het beleggen van verantwoordelijkheid op het gebied van informatieveiligheid binnen de organisatie. Zie hiervoor hoofdstuk 3.
- Informatieveiligheid is integraal onderdeel van het risicomanagement.
- Informatieveiligheid is een continu verbeterproces.
- Persoonsgegevens worden verwerkt volgens de AVG.
- De organisatie is transparant over de verwerking van persoonsgegevens.

Techniek

- Informatiesystemen zijn ingericht conform standaarden (bv. BIO, ISO 27000 serie, NEN DIV, GEMMA), worden beheerd conform standaarden (bv. ITIL/BiSL) en voldoen aan wet- en regelgeving (AVG, UAVG, AWB, WOO, Wob etc.).
- Het beheersen van de toegang tot informatiesystemen om onder andere ongeautoriseerde toegang tot gegevens te voorkomen.
- Het technisch beschermen van bedrijfsmiddelen door iedere medewerker en bestuurder.

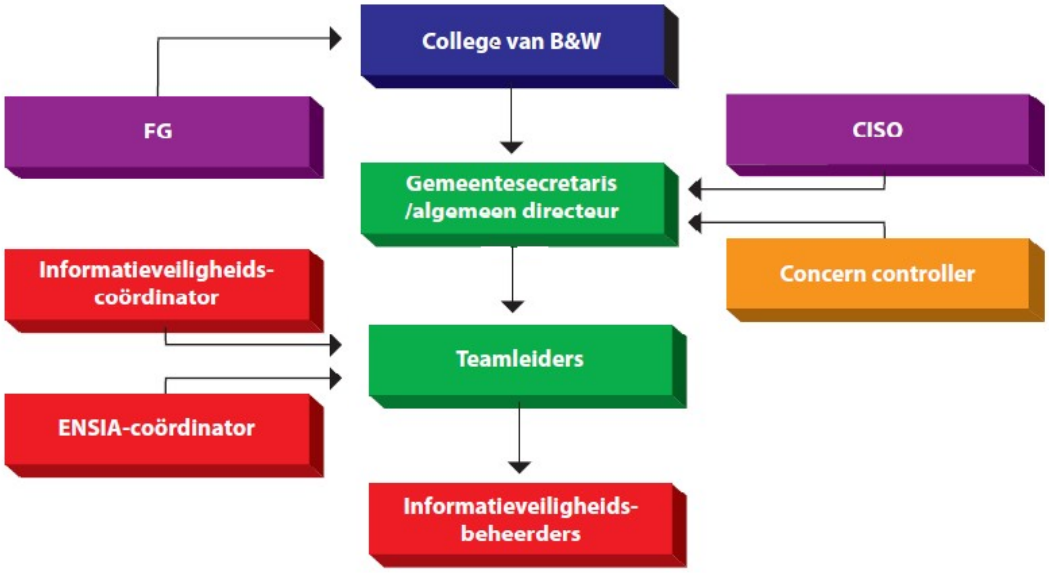
In bijlage 1 worden de hierboven genoemde uitgangspunten verder uitgewerkt voor de situatie in Doesburg.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt beschreven welke taken en verantwoordelijkheden met betrekking tot informatieveiligheid op welke plaats belegd zijn binnen de organisatie. Hierbij wordt de RASCI (Responsible, Accountable, Consulted, Supportive en Informed) methodiek gehanteerd. Op basis van deze 5 begrippen zijn de functies en rollen binnen de gemeente onderverdeeld.

Begrippen RASCI	Omschrijving
Responsible (Verantwoordelijk)	Responsible (R) staat voor verantwoordelijk. Dit is degene die verantwoordelijk is voor het werk dat gedaan moet worden. De persoon (of personen) 'doet' daadwerkelijk het werk, de taak of de activiteit. De R heeft de juiste middelen en bevoegdheden nodig om het werk goed uit te voeren.
Accountable (Eindverantwoordelijk)	Accountable (A) staat voor eindverantwoordelijk. De A is uiteindelijk eindverantwoordelijk voor de taak die R uitvoert. Deze persoon (of personen) wordt afgerekend op het resultaat.
Supportive (Ondersteunend)	Supportive (S) levert op verzoek van de R ondersteuning. De S is een expert op zijn of haar gebied en is alleen verantwoordelijk voor de kwaliteit van zijn support. Niet voor het eindresultaat.
Consulted (Raadplegen)	Consulted (C) is de persoon (of personen) die wordt geraadpleegd tijdens het proces. De C geeft de R advies over beslissingen of acties.
Informed (Informeren)	Informed (I) staat voor geïnformeerd. Deze persoon (of personen) wordt op de hoogte gehouden van de status en het resultaat van het werk.

Onderstaand een organogram van de Informatieveiligheidsorganisatie in Doesburg



In bijlage 2 is bovenstaand RASCI model verder uitgewerkt en ingevuld met de rollen, taken en verantwoordelijkheden in Doesburg.

4. Inrichting informatieveiligheidsprocedures

Dit informatieveiligheidsbeleid wordt op tactisch en operationeel niveau verder aangevuld met onderwerpspecifieke beleidsdocumenten, procedures en werkinstructies. Deze documenten worden afzonderlijk vastgesteld door het management. Onderstaand een overzicht van mogelijke onderwerpspecifieke documenten. Het overzicht is gebaseerd op producten uit de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Daarnaast is ook de verbinding gelegd met de specifieke vakgebieden van de gemeente.

Voor Suwinet staan de informatieveiligheidsprocedures en de rollen beschreven in het Aansluitbeleid SUWI Doesburg.

Figuur 5: Overzicht onderwerp specifieke documenten

5. Controle en verantwoording

De controle en verantwoording van informatieveiligheid valt in Doesburg uiteen in drie onderdelen:

- Informatiebeveiliging wordt getoetst via ENSIA op basis van de BIO;
- Informatiebeveiliging wordt ook getoetst door de directe rapportagelijn van de CISO naar de gemeentesecretaris / algemeen directeur;
- Over naleving van de AVG rapporteert de FG jaarlijks aan het college van B&W.

De verantwoordingsmomenten van deze drie onderdelen wordt zoveel als mogelijk op elkaar afgestemd in het kader van onze reguliere P&C cyclus met als belangrijk onderdeel de integrale voortgangsrapportage.

5.1 ENSIA

Het college van B&W verantwoordt zich jaarlijks over informatiebeveiliging door middel van de ENSIA zelfevaluatie. De ENSIA-coördinator vraagt de informatie die hiervoor nodig is op bij de procesverantwoordelijken. Op basis van de uitkomsten van de ENSIA zelfevaluatie stelt het college van B&W een collegeverklaring op. Daarin geeft het college van B&W aan in hoeverre de gemeente voldoet aan de normenkaders voor informatiebeveiliging. In de ENSIA verantwoording is ook een vragenlijst aanwezig over de AVG. Hierin worden de essentiële eisen uit de AVG door middel van een zelfevaluatievragenlijst getoetst.
Een onafhankelijke externe IT-auditor controleert de collegeverklaring en stelt een Assurance rapport op. Vervolgens rapporteert het college van B&W deze uitkomsten aan de gemeenteraad. De resultaten uit de collegeverklaring komen terug in het jaarverslag.

5.2 Informatiebeveiliging

De CISO heeft een directe rapportagelijn over de uitvoering van het informatieveiligheidsbeleid en het naleven van uitvoeringsrichtlijnen naar de gemeentesecretaris / algemeen directeur en de portefeuillehouder uit het college van B&W. In Doesburg streven we ernaar dat de verantwoording over Informatieveiligheid wordt geïntegreerd in de P&C cyclus en dat de jaarlijkse verantwoording plaatsvindt bij de jaarrekening.

5.3 Privacy

De FG rapporteert jaarlijks rechtstreeks aan het college van B&W over de mate waarin de gemeente de AVG naleeft. Daarvoor toetst de FG de organisatie onder andere via de informatieveiligheidscoördinator op het gebied van privacy. De rapportage bevat elementen waaruit duidelijk wordt op welke onderwerpen aan de AVG wordt voldaan en waar verbetering

nodig is. Hieruit volgen aanbevelingen waarbij de prioriteit is weergegeven. Door onderdelen die verbetering vereisen uit te voeren neemt de gemeente verantwoordelijkheid om aan de AVG te voldoen. De verantwoording over de stand van zaken m.b.t. privacy wordt geïntegreerd in de P&C cyclus en de jaarlijkse verantwoording gaat plaatsvinden bij de jaarrekening.

Bijlage 1 - Invulling uitgangspunten Doesburg

In deze paragraaf wordt voor de gemeente Doesburg verder invulling gegeven aan de uitgangspunten uit hoofdstuk 2.

Mens

- Iedere medewerker en bestuurder doet jaarlijks mee aan het bewustzijnstraject op het gebied van Informatieveiligheid. Doesburg heeft hiervoor structurele middelen gereserveerd en biedt jaarlijks activiteiten aan op dit gebied.
- Nieuwe medewerkers en bestuurders krijgen binnen 3 maanden een inwerkprogramma waar informatieveiligheid deel vanuit maakt. Leidinggevenden stimuleren dit en zien hierop toe. In Doesburg bieden we dit aan via onze digitale leeromgeving.
- Iedere medewerker en bestuurder meldt veiligheidsincidenten volgens de daarvoor vastgestelde procedure. Het melden kan eventueel ook anoniem bij de (externe) vertrouwenspersoon. In Doesburg is dit proces al ingebed in de organisatie. Meldingen worden gedaan via de Privacy coördinator, die jaarlijks over zijn bevindingen rapporteert aan portefeuillehouder en algemeen directeur.
- Iedere medewerker en bestuurder heeft voor indiensttreding een VOG. Dit is ingebed in de aanstellingsprocedure van P&O.
- Iedere medewerker en bestuurder kent de voor zijn of haar functie specifieke beleidsdocumenten en werkinstructies voor informatieveiligheid. In Doesburg wordt dit meegenomen in het (ICT) introductie programma.

Organisatie

- Alle processen met bijbehorende applicaties en gegevens in Doesburg hebben altijd minimaal 1 (proces)eigenaar. Dit gaan we vastleggen in ons ‘register van verwerkingen’.
- Deze eigenaar is primair verantwoordelijk voor de bescherming en juist gebruik van de informatie.
- De (proces)eigenaar bepaalt en onderbouwt de mate van bescherming van de bedrijfsprocessen. Dit beveiligingsniveau wordt vastgelegd in het ‘register van verwerkingen’.
- De (proces)eigenaar is integraal verantwoordelijk voor de uitvoering van de informatieveiligheid waaronder de ketens van informatiesystemen.
- Maatregelen voor informatieveiligheid worden genomen in relatie tot de grootte van een vermeend risico.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor informatieveiligheid n.a.v. de rapportages van de CISO en de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- Informatieveiligheid moet onderdeel gaan uitmaken van elk projectplan bij aanschaf of aanpassing van informatiesystemen en/of processen waarin gevoelige informatie wordt verwerkt.

- Door middel van een Information Security Management System (ISMS) wordt de kwaliteit van informatieveiligheid verhoogd. In Doesburg gaan we hiervoor Pepperflow inzetten.
- Persoonsgegevens worden alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel verwerkt. Dit doel wordt vastgelegd in het 'register van verwerkingen'.
- Er worden niet meer persoonsgegevens verwerkt en niet langer bewaart dan nodig om het doel te bereiken. Ook de bewaartermijnen worden vastgelegd in het 'register van verwerkingen'
- In het 'register van verwerkingen' worden alle processen met persoonsgegevens per categorie omschreven.
- Bij samenwerking met externe partijen leggen we afspraken over de informatieveiligheid vast indien er gevoelige gegevens uitgewisseld worden.
- Verzoeken met betrekking tot de rechten van betrokkenen op het gebied van de AVG kunnen zonder belemmeringen worden gedaan.
- We geven zo snel als mogelijk opvolging aan gemelde veiligheidsincidenten. Indien nodig melding van ernstige incidenten bij de Autoriteit Persoonsgegevens.
- Dit beleid wordt ieder jaar geëvalueerd en elke 3 jaar of bij een grote wijziging geactualiseerd.

Techniek

- Gebruikers hebben alleen toegang tot die informatie die ze nodig hebben voor de uitoefening van hun werk. Het betreft het principe 'gesloten, tenzij'.
- De proceseigenaar controleert periodiek dat alleen geautoriseerde medewerkers de relevante persoonsgegevens kunnen inzien en verwerken.
- Veilig mailen wordt technisch mogelijk gemaakt voor alle medewerkers volgens de NTA 7516 norm.

Bijlage 2 – Verdieping rollen, taken en verantwoordelijkheden

Verantwoordelijk – Responsible

Gemeentesecretaris / algemeen directeur

De gemeentesecretaris / algemeen directeur zorgt dat de verantwoordelijke portefeuillehouder binnen het college van B&W gevraagd en ongevraagd geïnformeerd wordt. Zo wordt B&W op de hoogte gehouden van het niveau van de informatieveiligheid binnen de organisatie. Hierover wordt de gemeentesecretaris / algemeen directeur geïnformeerd door de teamleiders, de CISO en de FG. Om inzicht te hebben en om keuzes te maken voor het vervolg stelt de gemeentesecretaris / algemeen directeur jaarlijks het Informatieveiligheidsplan (IVP) vast.

Teamleiders

De teamleiders dragen binnen hun team het Informatieveiligheidsbeleid en de daaraan gerelateerde onderwerp specifieke beleidsregels en procedures uit. Zoals bijvoorbeeld de procedure rondom beveiligingsincidenten en datalekken. Zij leggen hierover verantwoording af aan de gemeentesecretaris.

Het lijnmanagement laat zich periodiek informeren over de stand van zaken op het gebied van informatieveiligheid om relevante risicoafwegingen te kunnen maken.

Eindverantwoordelijk – Accountable

College van B&W

Het college van B&W is eindverantwoordelijk voor de informatieveiligheid. Zij stelt het Informatieveiligheidsbeleid en de daarbij behorende middelen vast. De gemeenteraad houdt hier toezicht op.

Ondersteunend - Supportive

Informatieveiligheidscoördinator (IVC)

De IVC ondersteunt de organisatie en teamleiders op tactisch en operationeel niveau met sjablonen, informatie, tips en rapportages door onder andere het:

- Jaarlijks opstellen van een informatieveiligheidsplan. Dit plan is gebaseerd op het informatieveiligheidsbeleid en uitgevoerde analyses. Denk hierbij aan een GAP analyse.
- Overleggen met de Informatieveiligheidsbeheerders over specifieke beleidsregels en procedures.
- Ondersteunen van de informatieveiligheidsbeheerders bij de uitvoering en implementatie van de specifieke beleidsregels en procedures.
- Bespreken van voorstellen en adviezen met de CISO of de FG.
- Verantwoording afleggen over de voortgang van de uitvoering van het informatieveiligheidsplan.
- Ook privacy coördinatie valt onder deze rol.

De rol van informatieveiligheidscoördinator heeft op drie specifieke deelgebieden een voorgeschreven officiële benaming. Het betreft de:

- Beveiligingsfunctionaris BRP (in Doesburg belegd bij team KCC)
- Beveiligingsfunctionaris reisdocumenten (in Doesburg belegd bij team KCC)
- Security Officer Suwinet (in Doesburg belegd bij team Staf)

In deze rol heeft de informatieveiligheidscoördinator de verantwoordelijkheid voor het toezicht op de naleving van de beveiligingsprocedures van de BRP, reisdocumenten en Suwinet.

ENSIA-coördinator

De ENSIA-coördinator coördineert of de beveiligingsorganisatie in overeenstemming is met de voorgeschreven ENSIA normen. De ENSIA-coördinator ondersteunt de sector specifieke medewerker bij het voldoen aan de gestelde ENSIA normen. Verder ondersteunt hij / zij het college van B&W bij het afleggen van horizontale verantwoording naar de gemeenteraad en verticale verantwoording naar de landelijke toezichthouders over informatieveiligheid en de uitvoering van de normenkaders BIO, Suwinet, DigiD en wetten BAG, BGT, BRO. In Doesburg is deze rol belegd bij team I&A).

Informatieveiligheidsbeheerders (IVB)

De informatieveiligheidsbeheerder draagt zorg voor het uitvoeren van de maatregelen binnen hun afdeling of team die volgen uit het informatieveiligheidsbeleid en - plan.
Zij signaleren incidenten op het gebied van informatieveiligheid in hun applicatie en verbonden processen. In de organisatie wordt deze rol vaak door de (functioneel) applicatiebeheerder ingevuld. Ook privacybeheer valt onder deze rol. Daarnaast is er voor een aantal deelgebieden een informatieveiligheidsbeheerder aangewezen met een officiële rolbenaming:

- Autorisatiebevoegde Reisdocumenten / Aanvraagstations
- Autorisatiebevoegde Rijbewijzen
- Beveiligingsbeheerder SUWI
- Beveiligingsbeheerder FZ
- Beveiligingsbeheerder P&O
- Beveiligingsbeheerder DigiD
- Beveiligingsbeheerder BAG
- Beveiligingsbeheerder BGT
- Beveiligingsbeheerder BRO
- Beveiligingsbeheerder DIV

In zijn bovenstaande rollen reeds belegd en ingebed in de organisatie.

Contactpersonen voor informatiebeveiliging

De informatiebeveiligingsdienst (IBD) ondersteunt gemeenten op het gebied van informatie-veiligheid. Hiervoor maakt de IBD gebruik van contactpersonen binnen de gemeente(n). De gemeente werkt met de onderstaande twee soorten contactpersonen.

Vertrouwde contactpersoon informatiebeveiliging (VCIB)

De VCIB is een contactpersoon binnen onze organisatie. Deze medewerker is in staat om de vertrouwelijke informatie die hij / zij krijgt van de IBD op waarde te kunnen schatten. De informatie die de IBD deelt met de VCIB is vertrouwelijk vanwege de aard en bron van de informatie. Deze rol is voor Doesburg belegd bij de teamleider ICT samenwerking en bij de Adviseur automatisering.

Algemene contactpersoon informatiebeveiliging (ACIB)

De ACIB is een contactpersoon binnen onze organisatie. Deze medewerker krijgt algemene waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten van de IBD. Deze rol is voor Doesburg belegd bij de Adviseur automatisering en de Servicedesk ICT samenwerking.

Raadplegen - Consulted

Chief Information Security Officer (CISO)

De CISO heeft een onafhankelijke positie tegenover zowel het management als het college van B&W. Hij / zij stelt doelen op voor informatieveiligheid die worden opgenomen in het informatieveiligheidsbeleid. Hij / zij geeft gevraagd en ongevraagd advies over informatieveiligheid aan het management op basis van risico gestuurd werken. De CISO is verbonden met de ambtelijke organisatie en heeft inzicht in het primaire proces.

Functionaris Gegevensbescherming (FG)

De FG heeft een onafhankelijke positie tegenover zowel het management als het college van B&W. Hij / zij geeft gevraagd en ongevraagd advies over de privacy en houdt toezicht op de privacy. De FG vertegenwoordigt de Autoriteit Persoonsgegevens als toezichthouder op de verwerking van persoonsgegevens binnen de gemeentelijke organisatie. De FG rapporteert jaarlijks het college van B&W over de uitvoering van het informatieveiligheidsbeleid via de

verantwoordingslijnen (P&C) met het accent op de juiste toepassing en interpretatie van de privacywetgeving. De gemeente Doesburg
heeft een regionale Functionaris Gegevensbescherming (FG) benoemd. De FG is de interne toezichthouder voor acht organisaties en de Autoriteit Persoonsgegevens (AP) is de externe toezichthouder.

Informeren - Informed

Concern controller

De concern controller richt zich op de planning en control (P&C cyclus) van financiën, processen, de doelmatigheid van beleid (zoals dit informatieveiligheidsbeleid) en doet dit op basis van risicomanagement. In de P&C cyclus is informatieveiligheid een structureel onderwerp.