GEMEENTE DOESBURG

Intern Informatieveiligheidsbeleid gemeente Doesburg

2023-2026

Datum: Februari 2023

Team: I&A

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	September 2022	R. Gerritsen A. Nas	Eerste herziening
1.0	November 2022	R. Gerritsen A. Nas	Actualisatie op basis van vernieuwde wetgeving, lessons learned en dreigingsbeeld(en).
1.1	Februari 2023	P. Stuart	Bestuurlijk voorwoord opgesteld en document aangepast op structuur en werkwijze Doesburg

Bestuurlijk Voorwoord

Regelmatig verschijnen er berichten in de media over bedrijven en instellingen die het slachtoffer zijn geworden van cybercriminaliteit. Grote en kleine bedrijven, scholen, ziekenhuizen en overheidsinstellingen, we hebben er allemaal mee te maken. Een gemeente als het Hof van Twente is inmiddels al twee jaar bezig om haar administratie en systemen opnieuw op te bouwen na een cyberaanval. De schade hiervan loopt inmiddels in de miljoenen Euro's.

We hebben inmiddels al lang niet meer te maken met amateurs die een stukje software schrijven om daarmee aandacht te krijgen. Het gaat hier om een reële dreiging vanuit criminele organisaties die een economisch verdienmodel hebben ontwikkeld om via kwaadaardige software toegang te krijgen tot onze informatiesystemen, om vervolgens onze systemen op slot te zetten en/of onze informatie openbaar te maken. Vervolgens wordt er gevraagd om een flink bedrag aan losgeld om de ontstane schade te herstellen. Een optie waar we als overheid niet in mee willen gaan want dan worden we medefinancier van de activiteiten van deze criminelen.

De IBD maakt in haar dreigingsbeeld voor de komende jaren, gericht aan de bestuurders van gemeenten, melding van een ernstige situatie. Het aantal digitale aanvallen op gemeenten neemt jaarlijks fors toe.
Op dit moment worden er vanuit de IBD wekelijks zo'n 15 meldingen gedaan van kwetsbaarheden die gevonden zijn in systemen van de gemeenten. Al deze meldingen moeten serieus bekeken worden en mogelijk moeten er acties ondernomen worden om de kwetsbaarheden op te lossen. Gemeenten zijn met name kwetsbaar omdat we met veel (gevoelige) informatie werken in veel verschillende systemen en ook nog eens in veel samenwerkingsverbanden met andere organisaties samenwerken.

Wat zijn de risico's van deze ontwikkelingen voor de gemeente?

Fouten in de dienstverlening
De kwaliteit en integriteit van data zijn van groot belang. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

Uitval van dienstverlening en bedrijfsvoering
Als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering. De burgers kunnen minder of niet meer op ons rekenen.

Vertrouwelijke informatie in verkeerde handen

Gemeenten verwerken voor hun wettelijke taken veel vertrouwelijke informatie. Onterechte toegang tot deze informatie kan uiterst nadelige gevolgen hebben voor inwoners en ondernemers. Een datalek of een overtreding van de AVG kan leiden tot hoge boetes voor de gemeente.

We moeten als gemeente anticiperen op bovenstaande ontwikkelingen en zorgen dat onze Informatieveiligheid goed op orde komt en betrouwbaar blijft. De basis hiervoor wordt gelegd in dit Informatieveiligheidsbeleid.

Maar met beleid alleen zijn we er niet. Om tegenwicht te bieden aan de toenemende bedreigingen in de komende jaren, moeten we blijven investeren in mensen en middelen. En dan gaat het niet alleen om onze technische beveiliging, maar ook in de kennis, houding en gedrag van medewerkers. Medewerkers worden steeds vaker geconfronteerd met valse berichten en worden verleid om informatie in te vullen of af te geven op onveilige websites. Digitale communicatie neemt enorm toe en ook de kans dat hierin iets misgaat. Bewustwording op dit gebied blijft een belangrijk aandachtspunt en kan niet langer vrijblijvend zijn. Daarnaast zullen we ons ook steeds meer moeten verantwoorden over de manier waarop onze informatievoorziening ingericht is, welke gegevens we waarom verwerken en of dit op een veilige manier gebeurt.

Leeswijzer

Dit beleid betreft een update van het huidige beleid dat vastgesteld was voor de periode van 2020 tot en met 2022. De wereld om ons heen veranderd continu en daarmee ook de context van de bedreigingen m.b.t. onze informatievoorzieningen. Daarnaast zijn ook organisatieontwikkelingen meegenomen in deze update van het beleid.

Het beleid is mede gebaseerd op normenkaders die vastgesteld zijn vanuit de overheid. Het gaat hierbij om de volgende normenkaders: De **Baseline Informatiebeveiliging Overheid (BIO)** en de **Algemene Verordening Gegevensbescherming (AVG/UAVG)**.

In hoofdstuk 1 wordt ingegaan op het begrip Informatieveiligheid en welke onderwerpen daar deel van uit maken. Ook wordt ingegaan op samenwerkingsverbanden.

In hoofdstuk 2 wordt verder ingegaan op de doelen en de scope van het beleid.
In paragraaf 2.4.2 worden de belangrijkste uitgangspunten verwoord.
De uitgangspunten zijn verdeeld in de categorieën **Mens, Organisatie** en **Techniek**.

In hoofdstuk 3 wordt verder ingegaan op de organisatie van onze Informatieveiligheid. Welke taken liggen bij wie op welk niveau en welke rollen onderscheiden we.

Om uitvoering te geven aan dit beleid zijn de algemene uitgangspunten verder ingevuld, zie hiervoor **bijlage 1**. Daarnaast zijn of worden er procedures en werkinstructies opgesteld voor specifieke onderwerpen, zoals voor de Basisregistratie Personen (BRP) en de Basisregistratie Adressen en Gebouwen (BAG).

Om te weten of we onze informatieveiligheid op orde hebben leggen we jaarlijks verantwoording af via de **verplichte ENSIA-audit en de AVG-toetsing**. Daarnaast rapporteert de CISO over de stand van zaken m.b.t. informatieveiligheid.

Met dit beleid willen we een vervolgstap zetten om de veiligheid van informatie en de bescherming van persoonsgegevens in onze organisatie verder te ontwikkelen. Om dit te kunnen realiseren hebben we iedereen nodig; **informatieveiligheid is van en voor ons allemaal!**

Inhoudsopgave

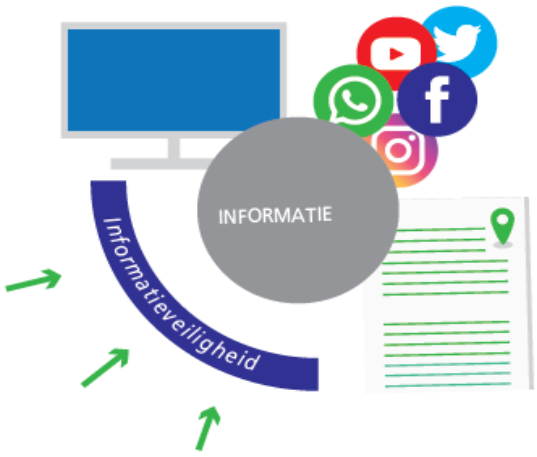
1. Inleiding

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

Als de veiligheid van informatie onvoldoende is gewaarborgd, ontstaan er risico's. Deze risico's spelen zich af bij de uitvoering van gemeentelijke taken en de continuïteit van de organisatie. Inbreuken op informatieveiligheid kunnen onder andere leiden tot financiële- en imagoschade.

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 aan analoge informatie op papier die 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 en daarmee op de veiligheid van onze inwoners

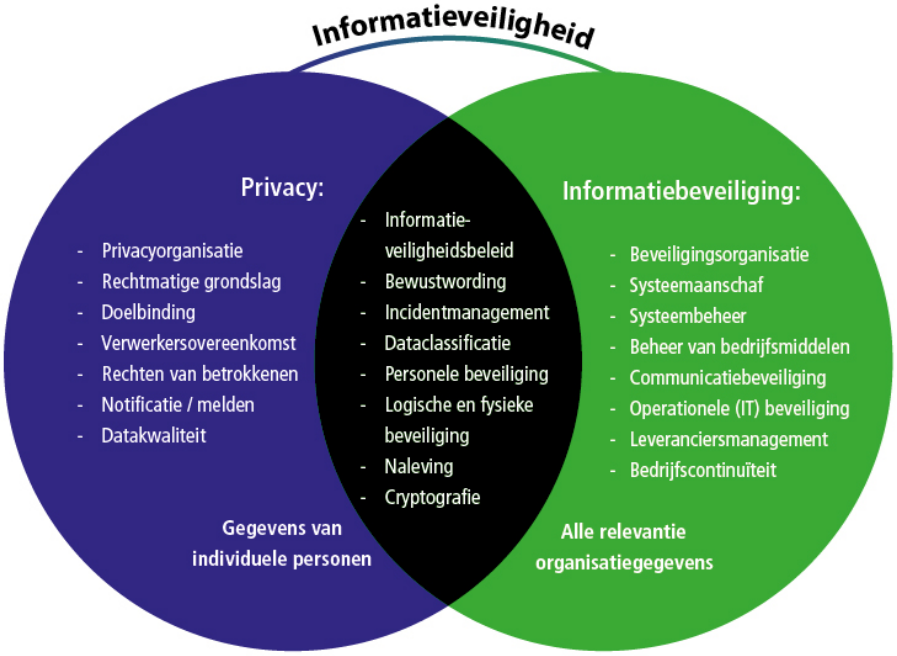


Figuur 1: Wat is informatieveiligheid

1.1.1. Relatie tussen informatiebeveiliging en privacy

Informatieveiligheid valt uiteen in informatiebeveiliging en privacy. Zowel informatiebeveiliging als privacy gaan over het beschermen, beheren en beheersen van informatie. Waarbij privacy specifiek aandacht vraagt voor zorgvuldig omgaan met persoonsgegevens, gaat het bij informatiebeveiliging juist om de bescherming van álle relevante informatie in de organisatie. De onderwerpen zijn nauw met elkaar verbonden. In figuur 2 is de relatie tussen deze onderwerpen weergegeven.

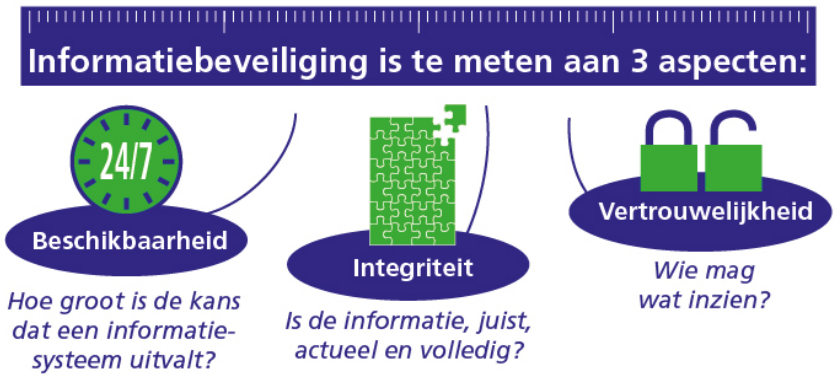
Om veilig met informatie om te gaan is dus aandacht nodig voor de beveiliging van informatie én voor het zorgvuldig omgaan met persoonsgegevens.



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 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.



Figuur 3: BIV aspecten

1.1.3. Privacy

Bij privacy gaat het om het zorgvuldig omgaan met persoonsgegevens. Een persoonsgegeven is alle informatie waarmee je uitkomt bij een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens van burgers worden voornamelijk verzameld voor onze

uitoefening van het openbaar gezag. Bij privacybescherming gaat het erom dat we in onze processen borgen dat er zorgvuldig omgegaan wordt met persoonsgegevens. Dat we een goede grondslag hebben voor de verwerking; dat we transparant zijn in wat we verwerken en dat we alleen die gegevens verwerken die voor het doel noodzakelijk zijn.
En mocht er een keer sprake zijn van een datalek dat we hier dan op een goede manier op reageren.

1.2. Samenwerkingsverbanden Informatieveiligheid

1.2.1. Regionale ICT samenwerking

Binnen ICT samen wordt er door de volgende organisaties samengewerkt: De gemeenten Aalten, Bronckhorst, Doesburg, Doetinchem, Oude IJsselstreek en de organisaties Buurtplein, BUHA, Erfgoedcentrum Achterhoek en Liemers, Laborijn, Omgevingsdienst Achterhoek, Regio Achterhoek/8RHK Ambassadeurs samen. Zij maken hierbij gebruik van de ICT-infrastructuur volgens het gastheerschapmodel, waarbij de gemeente Doetinchem optreedt als gastheer. Het gastheerschapmodel is vastgelegd op basis van een convenant en een dienstverleningsovereenkomst (DVO) tussen gemeente Doetinchem en de deelnemers.

Op het gebied van informatieveiligheid kennen we in het verlengde hiervan de volgende relevante overlegstructuren:

Naam overleg en invulling	Omschrijving
ICT-Automatiseringsoverleg *(Maandelijks overleg)*	In dit overleg worden ontwikkelingen besproken op tactisch niveau in de ICT-samenwerking door de ICT-contactpersonen van de gemeenten op het gebied van automatisering (fysieke ICT). Overige partners (niet gemeenten) mogen aansluiten, maar hebben geen besluitvormende stem.
Informatiseringsoverleg *(Maandelijks overleg)*	In dit overleg wordt bekeken welke ontwikkelingen samen kunnen worden verkend en opgepakt binnen de gestelde kaders van informatisering (o.a. applicatie keuze en inkooptrajecten).
Strategisch informatie-veiligheidsoverleg *(Zes-wekelijks overleg)*	Overleg tussen FG's en CISO's van de gemeentelijke organisaties die deelnemen aan de ICT-samenwerking. Dit overleg is vooralsnog informeel opgezet.
Privacy overleg *(Maandelijks overleg)*	In dit overleg worden privacy onderwerpen besproken, afgestemd en uitgewerkt tussen de privacy-coördinatoren en de FG. Er wordt kennis gedeeld en wordt gevraagd en ongevraagd advies gegeven.
Informatiebeveiligingsoverleg *(Zes-wekelijks overleg)*	In dit overleg worden informatiebeveiligingsonderwerpen besproken, afgestemd en uitgewerkt tussen de informatieveiligheidscoördinatoren. Het overleg heeft de rol om de veiligheid ter bescherming van informatie van de samenwerking te beheersen en te verbeteren. Daarnaast wordt ook gevraagd en ongevraagd advies gegeven aan verschillende stakeholders.

1.2.2. Regionale samenwerking veiligheidsregio

Naast de ICT-samenwerking hebben we op regionaal niveau ook te maken met de veiligheidsregio van de gemeente. Denk hierbij aan afspraken met de veiligheidsregio over inzet in het verlengde van de GRIP structuur bij mogelijke maatschappelijke gevolgen van een cyberaanval. De adviseur OOV speelt hierbij een belangrijke rol als linking pin naar de veiligheidsregio.

1.2.3. Landelijke samenwerking

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

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.

1.3. Ambitie en visie op informatieveiligheid

Dit informatieveiligheidsbeleid is onderdeel van de invulling van het Informatiebeleid van de gemeente Doesburg. De komende jaren zetten we in op verbetering van onze Informatieveiligheid en verdere professionalisering van de organisatie op dit gebied. Specifieke aandachtsgebieden voor de komende jaren zijn:

- De mens als eerste verdedigingslinie in alle lagen van de organisatie;
- Snel en adequaat kunnen reageren op incidenten;
- De continuïteit van de kritische bedrijfsprocessen;
- Inrichten volgens de principes security & privacy by design.
- (Blijven) voldoen aan geldende wetgeving, normen en audits;
- Groeien in het volwassenheidsniveau van onze beveiliging;

2. Strategisch beleid

2.1. Beleid

Dit beleid beschrijft de organisatie van de informatieveiligheid in de gemeente Doesburg voor de jaren 2023 tot en met 2026. Dit beleid vervangt het vastgestelde Informatieveiligheidsbeleid 2020-2022.
Dit beleid wordt in de organisatie in de praktijk verder aangevuld met onderwerp-specifieke documenten, procedures en werkinstructies die afzonderlijk worden vastgesteld door de procesverantwoordelijken. Zie hiervoor hoofdstuk 4.
Per kalenderjaar wordt een informatieveiligheidsplan (IVP) opgesteld waarin onderdelen uit dit beleid zijn uitgewerkt in concrete maatregelen.

2.2. Doelen

De doelen van het informatieveiligheidsbeleid zijn:

- Het beschermen van en op een 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.

2.3. Wetgeving en standaarden

Dit beleid is opgesteld op basis van wet- en regelgeving en verplicht gestelde normenkaders en een aanvulling op de meest actuele Informatievisie van de gemeente.

2.3.1. Informatiebeveiliging

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging voor de gehele overheid. Dit normenkader 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.

2.3.2. 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 alle daaraan gerelateerde regelgeving.

2.4. Scope

De scope van dit beleid omvat:

- alle gemeentelijke processen,
- alle onderliggende informatiesystemen,
- alle informatie-uitwisseling tussen de gemeente 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.

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

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Paspoorten en Nederlandse identiteitskaarten (PNIK)
- Digitale persoonsidentificatie (DigiD)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)

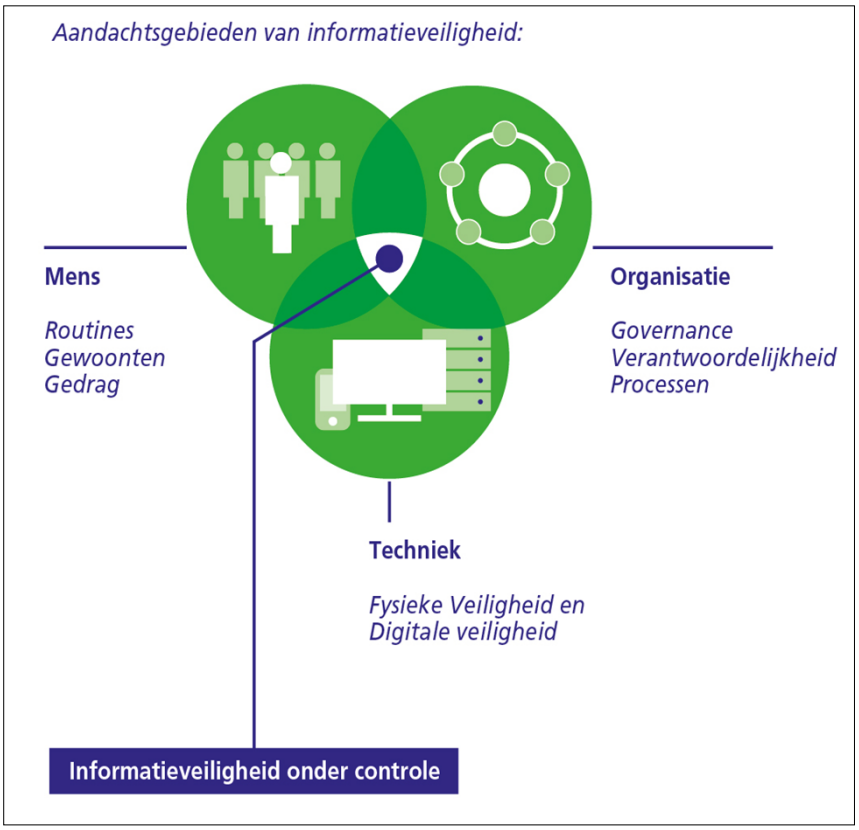
2.5. Uitgangspunten

Het college van burgemeester en wethouders, de gemeentesecretaris, de managers en teamleiders spelen een belangrijke rol bij het uitdragen en uitvoeren van dit beleid. Het management maakt een inschatting 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 een kapstok voor verschillende procedures zoals weergegeven in hoofdstuk 4.

2.5.1. Mens, Organisatie en Techniek

Bij informatieveiligheid gaat het om de bescherming van informatie in de breedste zin van het woord. Informatieveiligheid is meer dan alleen technisch verhaal en is daarmee ook niet van ICT. Door informatieveiligheid te benaderen vanuit de brede zin, via de aandachtsgebieden mens, organisatie en techniek, ontstaat een adequate bescherming van informatie.



Figuur 4 – Mens, Organisatie en Techniek

2.5.2. Algemene uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

Mens

- Iedereen[1] draagt bij aan het vergroten van bewustwording op het gebied van informatieveiligheid.
- Iedereen beschermt (persoons)gegevens tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- Iedereen meldt zo spoedig mogelijk een veiligheidsincident.

Organisatie

- Het college van burgemeester en wethouders is eindverantwoordelijk voor informatieveiligheid en stelt de benodigde mensen en middelen beschikbaar om dit beleid vast te stellen en uit te voeren.
- Leidinggevenden zijn integraal verantwoordelijk voor informatieveiligheid en de implementatie van dit beleid binnen de onderliggende teams. Zij bevorderen actief kennis en bewustzijn bij medewerkers.

[1] Onder iedereen wordt verstaan elke vaste, tijdelijke, interne, externe medewerker en elke bestuurder.

- Het verder uitbouwen en borgen van de informatieveiligheidsorganisatie (beveiliging en privacy) 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.
- Kritieke bedrijfsprocessen zijn onderbouwd bepaald en worden beschermd.
- Voor webapplicaties wordt informatie vastgelegd over onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.
- Informatieveiligheid is een continu verbeterproces.
- Persoonsgegevens worden verwerkt volgens de AVG.
- Bij besluitvorming is altijd sprake van menselijke tussenkomst.
- Er wordt geen gebruik gemaakt van profilering.
- 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, Archiefwet etc.).
- Het beheersen van de toegang tot informatiesystemen om ongeautoriseerde toegang tot gegevens te voorkomen.
- Het technisch beheren en beschermen van bedrijfsmiddelen.

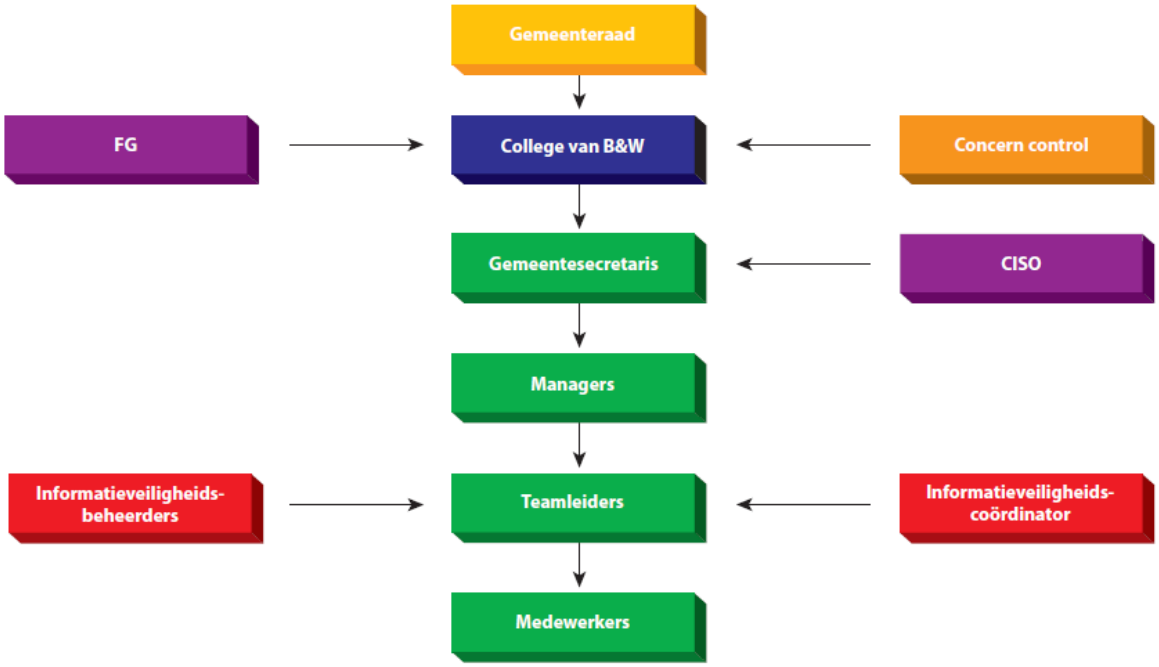
In bijlage 1 worden de hierboven genoemde uitgangspunten verder uitgewerkt voor de situatie in Doesburg!

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.

In bijlage 2 staan de rollen uitgebreid beschreven, ingedeeld volgens het RASCI model.



Figuur 5: Organogram met RASCI kleuren

N.b: In Doesburg is een organisatieontwikkeling gaande waarbij de Teamleiders mogelijk uit de lijn verdwijnen. In dat geval nemen de Managers ook de verantwoordelijkheden van de teamleiders op zich en worden ze daarin ondersteund door de IVB's en de IVC's.

4. Inrichting informatieveiligheidsprocedures

Dit informatieveiligheidsbeleid wordt verder aangevuld met onderwerpspecifieke beleidsdocumenten, procedures en werkinstructies. Deze documenten worden afzonderlijk vastgesteld door de verantwoordelijke op de betreffende vakafdelingen. In het onderstaande schematisch overzicht staat een globaal overzicht van deze onderwerpspecifieke documenten. Deze zijn 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 die worden benoemd in hoofdstuk 2.3.

Figuur 6: Overzicht onderwerp specifieke documenten

5. Controle en verantwoording

De controle en verantwoording van informatieveiligheid valt uiteen in onderstaande 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;
- Privacy (AVG) wordt jaarlijks getoetst door de FG, hierover wordt gerapporteerd aan het college van burgemeester en wethouders en verzoekt het college de gemeenteraad te informeren;
- Informatiebeveiliging en privacy zal worden ingebed in de P&C cyclus om zo ook risico's in beeld te brengen.

De verantwoordingsmomenten van deze onderdelen wordt zoveel als mogelijk op elkaar afgestemd.

5.1. ENSIA

Het college van burgemeester en wethouders verantwoordt zich jaarlijks over informatiebeveiliging door middel van de ENSIA zelfevaluatie. De ENSIA-coördinator vraagt informatie die hiervoor nodig is op bij de procesverantwoordelijken. Op basis van de uitkomsten van de ENSIA zelfevaluatie stelt de coördinator namens het college van burgemeester en wethouders een collegeverklaring op. Daarin geeft het college van burgemeester en wethouders aan in hoeverre de gemeente voldoet aan de normenkaders voor informatiebeveiliging. Verder ondersteunt de ENSIA-coördinator het college van burgemeester en wethouders 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. Een onafhankelijke externe IT-auditor controleert de collegeverklaring en stelt een assurance-rapport op. Vervolgens rapporteert het college van burgemeester en wethouders deze uitkomsten aan de gemeenteraad. De resultaten uit de collegeverklaring komen terug in een aparte verantwoording rondom de college verklaring.

5.2. Rapportage Informatiebeveiliging

De CISO heeft een directe rapportagelijn over de uitvoering van het informatieveiligheidsbeleid en het naleven van uitvoeringsrichtlijnen naar de gemeentesecretaris en de portefeuillehouder uit het college van burgemeester en wethouders. De CISO rapporteert jaarlijks over incidenten van het afgelopen jaar en de stand

van zake van de informatiebeveiliging. Als bron voor rapportage wordt ook gebruikt gemaakt van de resultaten van onze ENSIA audit en de updateverzoeken over Informatieveiligheid die twee keer per jaar door de managers ingevuld worden.

5.3. Privacy verantwoording

De FG rapporteert jaarlijks rechtstreeks aan het college van burgemeester en wethouders 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 wetgeving te voldoen.

Bijlage 1 - Uitgangspunten in Doesburg

In deze paragraaf wordt invulling gegeven aan de uitgangspunten uit hoofdstuk 2.

Mens

- Iedereen doet jaarlijks mee aan het bewustzijnstraject op gebied van informatieveiligheid;
- Nieuwe medewerkers en bestuurders krijgen binnen 3 maanden een introductie op het gebied van Informatieveiligheid aangeboden;
- Leidinggevenden stimuleren actief goed gedrag in het kader van informatieveiligheid en deelname aan bewustzijnstrajecten.
- Iedereen meldt veiligheidsincidenten volgens de daarvoor bestemde procedure. Het melden kan ook anoniem bij de (externe) vertrouwenspersoon;
- Iedereen kent de voor zijn of haar functie specifieke beleidsdocumenten en werkinstructies of helpt actief mee aan het opstellen hiervan in relatie tot informatieveiligheid.

Organisatie

- Door periodieke controle, organisatie-brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie;
- Alle processen, systemen, data, applicaties hebben altijd minimaal 1 (proces)eigenaar; deze is primair verantwoordelijk voor de bescherming en juist gebruik van de informatie. Deze bepaalt het risico op aantasting van de informatie en legt de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie vast;
- De proceseigenaar bepaalt en onderbouwt de mate van bescherming van de bedrijfsprocessen;
- De proceseigenaar is integraal verantwoordelijk voor de uitvoering van de informatieveiligheid waaronder de ketens van informatiesystemen;
- De proceseigenaar controleert periodiek dat alleen geautoriseerde medewerkers de juiste persoonsgegevens kunnen inzien en verwerken en legt deze controle vast;
- Maatregelen voor informatieveiligheid worden genomen in relatie tot de grootte van een vermeend risico en in beeld gebracht door middel van een (pre)-DPIA en/of dataclassificatie (BBN toets);
- Alle informatie in systemen met een DigiD-koppeling is geclassificeerd en kent een role based autorisatiemodel;
- Tijdens P&C-gesprekken met de leidinggevenden is het van belang om ook aandacht te hebben voor informatieveiligheid;
- Informatieveiligheid is een onderwerp in elk projectplan bij aanschaf of aanpassing van informatiesystemen en/of processen;
- Door middel van een Information Security Management System (ISMS) worden gegevens m.b.t. informatieveiligheid centraal vastgelegd.

- Persoonsgegevens worden alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel verwerkt, hiervoor is altijd een grondslag aanwezig;
- Er worden niet meer persoonsgegevens verwerkt en niet langer bewaard dan nodig om het doel te bereiken.
- De proceseigenaar omschrijft in het 'register van verwerkingen' alle processen waarbij persoonsgegevens verwerkt worden en houdt dit actueel;
- Bij samenwerking met externe partijen leggen we afspraken over de informatieveiligheid vast;
- 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;
- We stellen een plan op voor hoe te handelen bij een z.g. cybercrisis;
- Dit beleid wordt ieder jaar geëvalueerd en elke 4 jaar of bij een grote wijziging geactualiseerd;

Techniek

- Iedereen heeft slechts toegang tot die informatie die men nodig heeft voor de uitoefening van het werk. Het betreft het principe 'gesloten, tenzij';
- Iedereen kan gebruik maken van veilig mailen volgens NTA 7516 of de laatst geldende norm.
- We monitoren centraal onze ICT infrastructuur op verdachte activiteiten
- We maken gebruik van 2FA techniek voor de toegang tot onze digitale werkomgeving
- We zorgen voor backup voorziening voor onze centrale opgeslagen informatie
- We testen jaarlijks de veiligheid van onze centrale ICT systemen.
- We werken met centraal beheerde ICT apparatuur.

Bijlage 2 – Rollen, taken en verantwoordelijkheden in Doesburg

Verantwoordelijk – Responsible

Gemeentesecretaris/algemeen directeur

De gemeentesecretaris is verantwoordelijk voor de informatieveiligheid binnen de gemeentelijke organisatie. Hij zorgt dat de verantwoordelijke portefeuillehouder binnen het college van B&W gevraagd en ongevraagd geïnformeerd wordt over dit onderwerp. Zo blijft deze op de hoogte van het niveau van de informatieveiligheid binnen de organisatie. De gemeentesecretaris wordt geïnformeerd door de managers/teamleiders en door de CISO. Om inzicht te hebben en om keuzes te maken voor het vervolg wordt de gemeentesecretaris jaarlijks betrokken in de verantwoordingscyclus m.b.t. ENSIA en de AVG jaarrapportage. Ook stelt hij jaarlijks het Informatieveiligheidsplan (IVP) vast dat door de CISO opgesteld wordt.

Managers

Informatieveiligheid valt onder de integrale verantwoordelijkheid van de managers.
De managers zijn verantwoordelijk voor het (laten) uitvoeren van dit beleid en de onderwerp specifieke beleidsregels en procedures aanvullend op dit beleid. Hierover leggen zij verantwoording af aan de gemeentesecretaris. De managers zien erop toe dat de teamleiders en medewerkers adequate maatregelen nemen voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.

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 en de clean desk policy. Zij leggen hierover verantwoording af aan de managers. Indien er in de lijn geen teamleider aanwezig is, vallen deze verantwoordelijkheden onder de verantwoordelijkheid van de betreffende Manager.

Medewerkers

Hoewel de integrale verantwoordelijkheid in de hiërarchische lijn is belegd, is iedere medewerker in zekere mate ook zelf verantwoordelijk voor het juist en veilig gebruik van apparatuur en de informatie die hierbij wordt gebruikt of verwerkt. De medewerkers verantwoordelijk voor het volgen van geldende afspraken, zoals het vergrendelen van de werkplek, juist gebruik van eigen autorisaties en melden van verdachte situaties of datalekken.

Eindverantwoordelijk – Accountable

College van B&W

Het college van B&W is eindverantwoordelijk voor de informatieveiligheid. Zij stelt het Informatieveiligheidsbeleid vast. Om hier uitvoering aan te kunnen geven doet zij een voorstel voor de benodigde middelen bij de gemeenteraad.

Ondersteunend - Supportive

Informatieveiligheidscoördinator (IVC)

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

- 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.
- Zorgen voor realisatie van het informatieveiligheidsplan.
- Coördineren van de ENSIA audit en verantwoording.

In Doesburg wordt deze rol met name vervuld door de privacy coördinator en de adviseur automatisering.

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

- Beveiligingsfunctionaris BRP
- Beveiligingsfunctionaris reisdocumenten
- Security Officer Suwinet

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

Informatieveiligheidsbeheerders (IVB)

De informatieveiligheidsbeheerder draagt op operationeel niveau binnen zijn/haar team zorg voor het uitvoeren van de maatregelen die volgen uit het informatieveiligheidsbeleid en -plan. Hij/Zij signaleert incidenten op het gebied van informatieveiligheid in de applicatie en verbonden processen.
In Doesburg vervullen met name de Functioneel applicatiebeheerders deze rol. Ook is er een medewerker privacybeheer aangesteld voor een beperkt aantal uren.

Contactpersonen voor informatiebeveiliging

De informatiebeveiligingsdienst (IBD) ondersteunt gemeenten op het gebied van informatieveiligheid. 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. De teamleiders van ICT-Samen en van I&A, en de A-adviseur zijn VCIB.

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. De A-adviseur en de Servicedesk ICT zijn ACIB.

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 van de gemeente.
- De CISO 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.
- Jaarlijks stelt de CISO een informatieveiligheidsplan (IVP) op en laat dit vaststellen door de gemeentesecretaris.
  Dit plan is gebaseerd op het informatieveiligheidsbeleid en uitgevoerde analyses en audits.

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

Gemeenteraad

De gemeenteraad beslist over aangevraagde middelen in de begroting en houdt toezicht op de uitvoering van het informatieveiligheidsbeleid. Zij bepaalt op hoofdlijnen het informatieveiligheidsbeleid, zoals het voldoen aan de vigerende wet- en regelgeving.

Concern control

De concern control richt zich op de planning en control (P&C cyclus) van financiën, processen en zal ook het risicomanagement verder vormgeven. Hierdoor krijgt informatieveiligheid een meer structureel karakter.