gemeente [gD] Doetinchem

Informatieveiligheidsbeleid gemeente Doetinchem

Privacy- en Informatiebeveiligingsbeleid

2023-2026

Datum: november 2022

Team: Informatiemanagement

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	September 2022	R. Gerritsen A. Nas	Eerste herziening
1.0	Januari 2023	R. Gerritsen A. Nas	Actualisatie op basis van vernieuwde wetgeving, lessons learned en dreigingsbeeld(en).
1.1	April 2023	R. Gerritsen A. Nas	Aanpassingen gedaan op basis van feedback vanuit MT.

Samenvatting

De gemeente verwerkt veel gegevens om haar taken goed uit te voeren. Inwoners, bedrijven, ketenpartners en onze eigen medewerkers moeten erop kunnen vertrouwen dat informatie die wij verwerken betrouwbaar is én dat wij zorgvuldig omgaan met gegevens. Dit gaat ook over cruciale systemen en gemeentelijke processen (bruggen, sluis). Hiervoor is inzet van ons allemaal nodig.

Om privacy van inwoners en belangrijke systemen te beschermen 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 hiernaar 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 hebben wij uitgangspunten opgesteld, zie hiervoor bijlage 1. Daarnaast zijn er procedures en werkinstructies opgesteld voor specifieke onderwerpen, zoals voor de Basisregistratie Personen (BRP) en de Basisregistratie Adressen en Gebouwen (BAG). Hiervoor gebruiken wij de voorbeelden van onder andere VNG Realisatie en de Informatiebeveiligingsdienst (IBD).

Om inzicht te krijgen of we dit onderwerp goed oppakken leggen we jaarlijks verantwoording af via de **verplichte ENSIA audit**, **AVG toetsing en Wpg audit**.

Met dit beleid zetten we een volgende stap om de veiligheid van informatie en de bescherming van persoonsgegevens verder ontwikkelen. Om dit te realiseren hebben we iedereen nodig; **informatieveiligheid is van ons allemaal!**

Inhoudsopgave

Leeswijzer

In hoofdstuk 1 wordt toegelicht wat informatieveiligheid behelst en de onderlinge relatie tussen informatiebeveiliging en privacy en worden de doelen en scope van dit beleidsstuk beschreven.

De inrichting van de informatieveiligheidsorganisatie wordt in hoofdstuk 2 beschreven en hoe de taken en verantwoordelijkheden in deze zijn belegd.

Vervolgens wordt in hoofdstuk 3 wordt beschreven op welke wijze er regionaal en landelijk wordt samengewerkt.

Hoofdstuk 4 is het strategisch beleid toegelicht. Allereerst wordt beschreven welke ambities de gemeente Doetinchem nastreeft op gebied van informatieveiligheid en welke wet- en regelgeving van toepassing is. Vervolgens is het beleid verwoord in diverse uitgangspunten en de inrichting van de informatieveiligheidsprocedures.

Tot slot wordt in hoofdstuk 5 beschreven op welke wijze getoetst wordt of de informatieveiligheid conform wet- en regelgeving op orde is en op welke wijze hierover verantwoording wordt afgelegd.

1. Inleiding

De gemeente Doetinchem heeft een maatschappelijke verantwoordelijkheid: inwoners, 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. De veiligheid van informatie en het beschermen van gegevens neemt dan ook een belangrijke plek in.

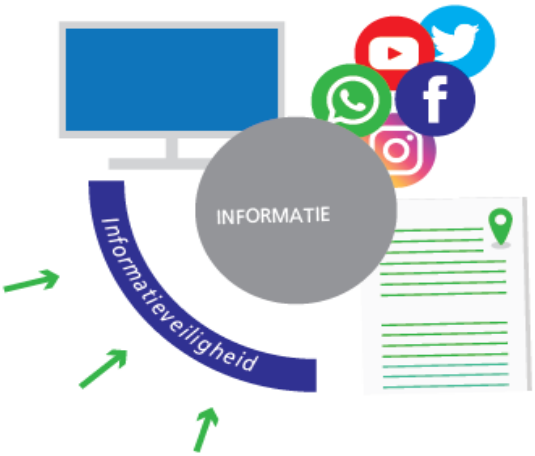
Wij geven prioriteit aan een digitaal weerbare gemeente. We zetten ons in om te voorkomen dat inwoners en bedrijven slachtoffer worden van cybercrime en gedigitaliseerde criminaliteit. Ook zorgen we ervoor dat de informatiebeveiliging van de gemeente op orde is en dat we goed voorbereid zijn op cybercrises en online aangejaagde ordeverstoringen. Informatieveiligheid is dan ook geen doel op zich, maar een continu groeiproces.

Als de veiligheid van informatie onvoldoende is gewaarborgd, kunnen er risico's ontstaan. 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 reputatieschade voor inwoners of financiële schade voor de organisatie. Kortom: informatieveiligheid is van ons allemaal.

Dit beleid beschrijft de informatieveiligheid van de gemeente Doetinchem voor de jaren 2023 tot en met 2026. Dit beleid vervangt het vastgestelde Informatieveiligheidsbeleid 2020-2022.

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 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 verkleint de kans op schade die van invloed is op de kwaliteit van het functioneren van de gemeente.

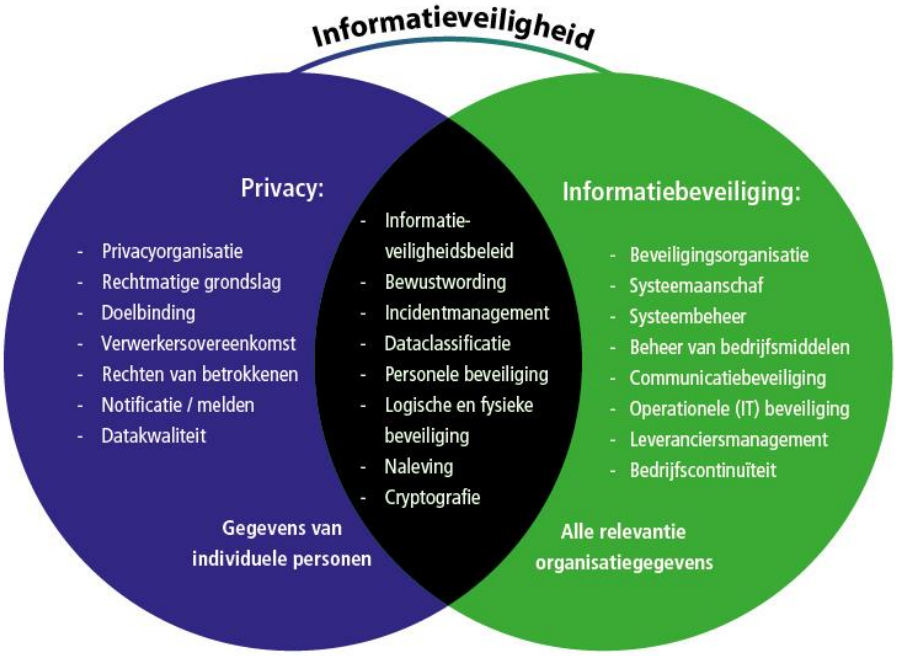


Figuur 1: Wat is informatieveiligheid

1.1.1. Relatie tussen informatiebeveiliging en privacy

Informatieveiligheid bestaat uit informatiebeveiliging en privacy. Zowel informatiebeveiliging als privacy gaat over het beschermen, beheren en beheersen van informatie. Waarbij privacy specifiek aandacht vereist voor zorgvuldig omgaan met persoonsgegevens. Bij informatiebeveiliging gaat het juist om de bescherming van álle relevante informatie. Beide onderwerpen zijn nauw met elkaar verbonden. In figuur 2 is de relatie tussen deze onderwerpen weergegeven.

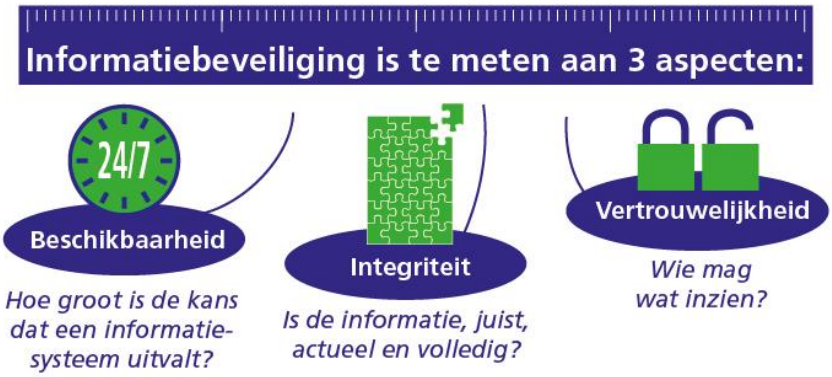
Om veilig met informatie om te gaan is aandacht nodig voor de beveiliging van informatie én het zorgvuldig omgaan met persoonsgegevens.



Figuur 2 – Verbondenheid privacy en informatiebeveiliging

1.1.2. Informatiebeveiliging

Bij informatiebeveiliging is de betrouwbaarheid van informatie belangrijk omdat dit de basis vormt voor het uitvoeren van gemeentelijke taken. Derhalve wil de gemeente zorgvuldig met gegevens omgaan. Dit doen we door de risico's te bepalen, daarom classificeren wij onze data (dataclassificatie, zie ook figuur 2). Dit wordt bepaald met behulp van drie aspecten, namelijk de mate van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Afhankelijk van het risico worden maatregelen toegepast.



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 inwoners worden voornamelijk verzameld voor onze taak in het kader van de uitoefening van het openbaar gezag (rechtmatige grondslag, zie ook figuur 2). De inwoner moet er op kunnen vertrouwen dat wij zorgvuldig en veilig met persoonsgegevens omgaan. Iedereen heeft recht op privacy.

1.2. 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.

1.3. 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 deze onderstaande vakgebieden specifieke beveiligingseisen. Deze worden in aparte documenten beschreven.

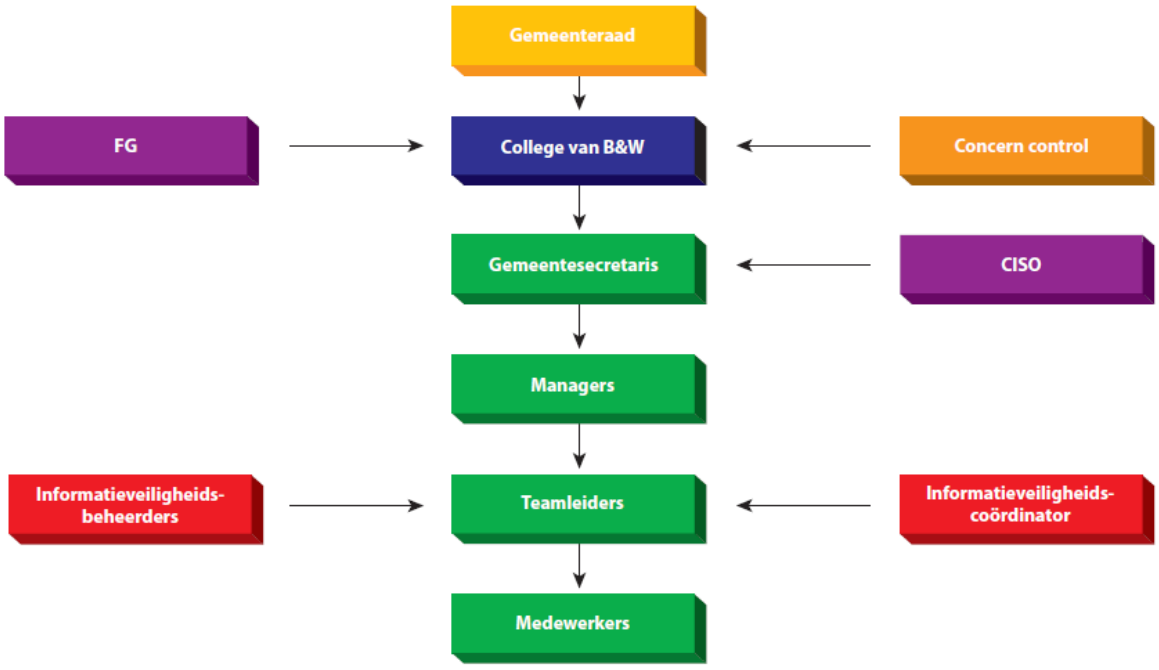
- Basisregistratie Personen (BRP);
- Paspoortuitvoeringsregeling (PUN);
- Paspoorten en Nederlandse identiteitskaarten (PNIK);
- Digitale persoonsidentificatie (DigiD);
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet);
- Basisregistratie Adressen en Gebouwen (BAG);

- Basisregistratie Grootschalige Topografie (BGT);
- Basisregistratie Ondergrond (BRO);
- Basisregistratie Waardering Onroerende Zaken (WOZ).

2. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt beschreven welke taken en verantwoordelijkheden met betrekking tot informatieveiligheid en 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. In bijlage 2 is het RASCI model nader toegelicht.

2.1. Organisatie



Een toelichting op de bovenstaande figuur is te lezen in de onderstaande paragraaf en in bijlage 2 van dit beleid.

2.1.1. Taken en verantwoordelijkheden

Verantwoordelijk - Responsible

Gemeentesecretaris/algemeen directeur

De gemeentesecretaris/algemeen directeur zorgt dat de verantwoordelijke portefeuillehouders binnen het college van burgermeester en wethouders gevraagd en

ongevraagd geïnformeerd worden. Zo zijn zij op de hoogte van het niveau van de informatieveiligheid binnen de organisatie. Hierover wordt de gemeentesecretaris/algemeen directeur geïnformeerd door de CISO, FG en de managers. Om inzicht te hebben en om keuzes te maken voor het vervolg stelt de gemeentesecretaris/algemeen directeur jaarlijks het Informatieveiligheidsplan (IVP) en de handboeken Informatieveiligheid voor DigiD, Suwinet en BRP vast.

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/algemeen directeur. De managers zien erop toe dat de teamleiders en medewerkers adequate maatregelen nemen voor de bescherming van de gegevens die onder hun verantwoordelijkheid vallen.

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 managers.

De managers en teamleiders voeren, eventueel met ondersteuning van de informatieveiligheidscoördinator(en), quick-scans uit op het gebied van informatieveiligheid om relevante risicoafwegingen te kunnen maken.

Medewerkers

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

Eindverantwoordelijk - Accountable

College van burgermeester en wethouders

Het college van burgermeester en wethouders 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

Informatieveiligheidscoördinatoren (IVC)

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

- Jaarlijks opstellen van een informatieveiligheidsplan. Dit plan is gebaseerd op het informatieveiligheidsbeleid en uitgevoerde analyses.
- 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/FG.
- Rapporteren over de voortgang van de uitvoering van het informatieveiligheidsplan. Coördineren van de ENSIA (zie ook paragraaf 5.1), (pre)DPIA's, register van verwerkingen.

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. De IVB signaleert incidenten op het gebied van informatieveiligheid in de applicatie en verbonden processen. In de organisatie wordt deze rol vaak door de (functioneel) applicatiebeheerder ingevuld. Daarnaast is er voor een aantal deelgebieden een informatieveiligheidsbeheerder aangewezen met een officiële rolbenaming:

- Autorisatiebevoegde Reisdocumenten/Aanvraagstations
- Autorisatiebevoegde Rijbewijzen
- Beveiligingsbeheerder SUWI
- Beveiligingsbeheerder FZ
- Beveiligingsbeheerder HR
- Beveiligingsbeheerder DigiD
- Beveiligingsbeheerder BAG
- Beveiligingsbeheerder BGT
- Beveiligingsbeheerder BRO
- Beveiligingsbeheerder archief
- Beveiligingsbeheerder WOZ

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 organisatie 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 ICT-Samenwerking en Informatiemanagement, ICT-beveiligingscoördinator en de CISO 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 informatieveiligheidscoördinatoren 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 burgermeester en wethouders. De CISO stelt doelen op in samenwerking met andere informatieveiligheidsfunctionarissen voor informatieveiligheid die worden opgenomen in het informatieveiligheidsbeleid. De CISO geeft gevraagd en ongevraagd advies over informatieveiligheid aan het management op basis van risico gestuurd werken en rapporteert hierover jaarlijks aan de gemeentesecretaris. De CISO is verbonden met de ambtelijke organisatie, heeft inzicht in het primaire proces en heeft een directe escalatielijn naar de gemeentesecretaris op het moment dat er zich misstanden voordoen waardoor de informatiebeveiliging in het geding komt.

Functionaris Gegevensbescherming (FG)
De FG heeft een onafhankelijke positie tegenover zowel het management als het college van burgermeester en wethouders. De FG geeft gevraagd en ongevraagd advies over de privacy, houdt toezicht op de naleving van de privacywetgeving en heeft een directe escalatielijn naar de gemeentesecretaris op het moment dat er zich misstanden voordoen waardoor de privacy in het geding komt. De FG vertegenwoordigt de Autoriteit Persoonsgegevens als toezichthouder op de verwerking van persoonsgegevens binnen de gemeentelijke organisatie. De FG rapporteert jaarlijks het college van burgermeester en wethouders over de uitvoering van het informatieveiligheidsbeleid via de verantwoordingslijnen (P&C) met het accent op de juiste toepassing en interpretatie van de privacywetgeving. De Autoriteit Persoonsgegevens (AP) is de externe toezichthouder. In het uiterste geval, waarbij de FG grote zorgen heeft over bewuste niet-naleving van de AVG, meldt de FG dit bij de AP.

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 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 in deze beleidsperiode ook het risicomanagement verder vormgeven.

3. Samenwerkingen

We staan er niet alleen voor. Zowel landelijk als regionaal zijn er initiatieven waar wij bij aangesloten zijn. Zo bundelen we kennis en krachten. De gemeente Doetinchem werkt in verschillende verbanden samen om informatieveiligheid te vergroten. Regionaal, via de ICT-samenwerking en door samenwerkingen met landelijke organisaties.

3.1. Regionale samenwerking

Binnen de Achterhoek wordt in diverse verbanden en samenstellingen met elkaar samengewerkt. Zo werken 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. Daarnaast wordt ook samengewerkt met gemeenten Winterswijk, Oost-Gelre, Montferland, Zutphen en Berkelland.

Op het gebied van informatieveiligheid bestaan 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 met de gemeentelijke partners wordt bekeken welke updates en ontwikkelingen samen kunnen worden verkend en opgepakt binnen de gestelde kaders van informatisering (o.a. applicatie keuze en inrichting).
Strategisch informatieveiligheids-overleg (Zes-wekelijks overleg)	Overleg tussen FG's en CISO's van de gemeentelijke organisaties aan de ICT-samenwerking. Dit overleg is vooralsnog informeel opgezet.
Regionaal FG overleg	In dit overleg bespreken regionale FG's actualiteiten en ontwikkelingen rondom privacy, om kennis te delen en elkaar te versterken/afstemmen.
Privacy overleg (Maandelijks overleg)	In dit overleg worden privacy onderwerpen besproken, afgestemd en uitgewerkt tussen de

	informatieveiligheidscoördinatoren en de FG. Kennis gedeeld en wordt gevraagd en ongevraagd advies gegeven aan overlegorganen en aan de gemeentesecretaris.
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.

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) 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.

4. Strategisch beleid

4.1. Ambitie op het gebied van informatieveiligheid

Dit informatieveiligheidsbeleid hangt samen met de Informatievisie. De komende jaren zet de gemeente Doetinchem in op het verhogen van Informatieveiligheid en verdere professionalisering van de organisatie op dit gebied. Aandachtsgebieden hierbij zijn:

- Blijven voldoen geldende wetgeving, normen en audits;
- Groeien in het volwassenheidsniveau[1];
- De mens als eerste verdedigingslinie in alle lagen van de organisatie;
- Snel en adequaat kunnen reageren, voorkomen en leren van incidenten;
- Het kunnen continueren van de kritische bedrijfsprocessen;
- Inrichten volgens de principes security & privacy by design.

4.2. 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.

4.2.1. Informatiebeveiliging

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

4.2.2. 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), de Wet politiegegevens (Wpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren (BpgBoa) en alle daaraan gerelateerde regelgeving.

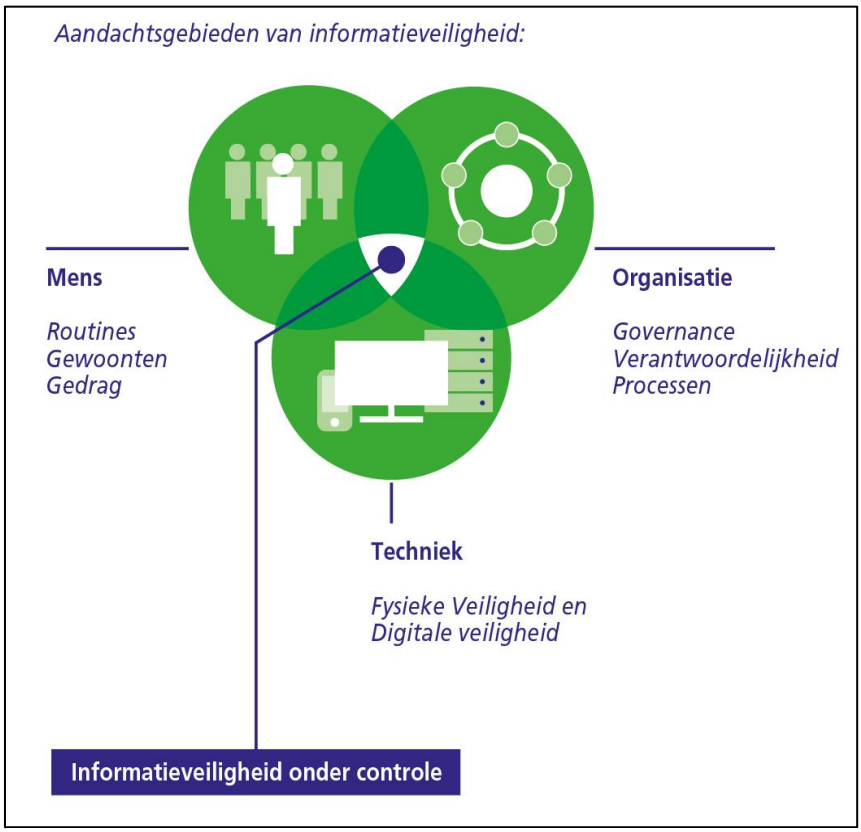
[1] Door middel van een model wordt het huidige volwassenheidsniveau (op een schaal van 1 tot 5) bepaald en welke stappen de organisatie kan zetten om het volwassenheidsniveau te verhogen.

4.3. Mens, Organisatie en Techniek

Het college van burgemeester en wethouders, de gemeentesecretaris, managementteam 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 risico's zij accepteert en op welke risico's maatregelen worden getroffen.

Dit beleid is van toepassing op de hele organisatie, alle processen, organisatieonderdelen, objecten, informatievoorzieningen, -systemen en gegevens(verzamelingen). Het is een kapstok voor verschillende procedures zoals weergegeven in paragraaf 4.4. De procedures worden periodiek bijgesteld door de proceseigenaren op basis van nieuwe ontwikkelingen, registraties in het incidenten- en datalekregister en risicoanalyses (zoals DPIA's).

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 technisch verhaal en is daarmee ook niet van ICT. Door informatieveiligheid te benaderen vanuit de aandachtsgebieden mens, organisatie en techniek, krijgt het de noodzakelijke aandacht in de volle breedte van onze organisatie. In het Informatieveiligheidsplan (IVP) worden acties beschreven om de voorgenoemde ambities en onderstaande uitgangspunten te realiseren of verder vorm te geven. Dit plan wordt jaarlijks opgesteld op basis van resultaten uit onder andere audits, rekenkameronderzoeken,

toetsingen en actualiteiten. In het IVP wordt ook beschreven of additionele middelen voor de uitvoering benodigd zijn.

De belangrijkste uitgangspunten van dit beleid zijn:

Mens
- Iedereen[2] helpt de bewustwording op het gebied van informatieveiligheid te vergroten.
- Iedereen beschermt gegevens tegen ongeautoriseerde toegang, -gebruik, -verandering, -openbaring, -vernietiging, -verlies of -overdracht.
- Iedereen meldt per omgaande 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.
- Managers en teamleiders zijn integraal verantwoordelijk voor informatieveiligheid en de implementatie van dit beleid binnen het team. Zij bevorderen actief kennis en bewustzijn bij medewerkers.
- Voor de informatieveiligheidsorganisatie (beveiliging en privacy) hebben we verschillende functionarissen nodig, waaronder een Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG), informatieveiligheidscoördinatoren en -beheerders.
- Informatieveiligheid is integraal onderdeel van het risicomanagement.
- Kritieke bedrijfsprocessen zijn onderbouwd bepaald en worden beschermd.
- Voor (web)applicaties handboeken informatieveiligheid opstellen met daarin onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.
- Informatieveiligheid is een continu verbeterproces.
- Wij verwerken persoonsgegevens volgens de AVG en Wpg.
- Wij doen niet aan automatische besluitvorming, tenzij hier een uitzondering voor geldt.
- Wij profileren niet, behalve als we daarmee past binnen geldende wet- en regelgeving.
- Wij verwerken bijzondere persoonsgegevens in daarvoor aangewezen applicaties.
- Wij zijn 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, Wpg, BpgBoa, Archiefwet etc.).

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

- We beheersen de toegang tot informatiesystemen om onder andere ongeautoriseerde toegang tot gegevens te voorkomen.
- Iedereen beschermt bedrijfsmiddelen.

In bijlage 1 worden de hierboven genoemde uitgangspunten verder uitgewerkt.

4.4. Inrichting informatieveiligheidsprocedures

Dit informatieveiligheidsbeleid wordt verder aangevuld met onderwerpspecifieke beleidsdocumenten, handboeken informatieveiligheid, procedures en werkinstructies. Deze (schriftelijk) documenten worden afzonderlijk vastgesteld. In het onderstaande schematisch overzicht staat een overzicht van deze onderwerpspecifieke documenten. Voor DigiD en Suwinet wordt jaarlijks beoordeeld of de handboeken informatieveiligheid moeten worden aangepast en opnieuw vastgesteld door de algemeen directeur. Deze zijn gebaseerd op producten uit de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) en Wet politiegegevens (Wpg). Daarnaast is ook de verbinding gelegd met de specifieke vakgebieden die worden benoemd in paragraaf 1.3.

Figuur 5: 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 CISO. Hierover rapporteert de CISO direct naar de gemeentesecretaris/algemeen directeur;
- Privacy wordt jaarlijks getoetst (AVG en Wpg) door de FG, hierover wordt gerapporteerd aan het college van burgemeester en wethouders en verzoekt het college de gemeenteraad te informeren;
- Informatieveiligheid zal worden ingebed in de P&C cyclus om elk kwartaal risico's in beeld te brengen;
- Met behulp van een ISMS/PMS wordt de kwaliteit van informatieveiligheid gemonitord.

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 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 assurancerapport 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. Informatiebeveiliging

De CISO heeft een directe rapportagelijn over de uitvoering en naleving van het informatieveiligheidsbeleid naar de gemeentesecretaris/algemeen directeur en de

portefeuillehouder uit het college van burgemeester en wethouders. Dit wordt gedaan voordat de P&C-gesprekken worden gevoerd. De CISO rapporteert jaarlijks.

5.3. Privacy

De FG rapporteert jaarlijks schriftelijk rechtstreeks aan het college van burgemeester en wethouders over de mate waarin de gemeentelijke organisatie de AVG en de Wpg naleeft. Daarvoor toetst de FG de organisatie onder andere via de informatieveiligheidscoördinatoren op het gebied van privacy. De rapportage bevat elementen waaruit duidelijk wordt op welke onderwerpen aan de AVG en Wpg 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 organisatie verantwoordelijkheid om aan de wetgeving te voldoen.

Daarnaast voeren voor de Wpg de proceseigenaren jaarlijks een interne audit uit en audit een onafhankelijke externe IT-auditor hen één keer per 4 jaar op de naleving van de Wpg De rapportage van de externe audit moet naar de Autoriteit Persoonsgegevens worden gestuurd.

Bijlage 1 - Invulling uitgangspunten

In deze bijlage wordt invulling gegeven aan de uitgangspunten uit hoofdstuk 4.

Mens

- Iedereen doet jaarlijks mee aan een bewustzijnstraject;
- Nieuwe medewerkers en bestuurders krijgen binnen 3 maanden een inwerkprogramma waar bewustwording ook deel van uit maakt;
- Managers en teamleiders stimuleren actief het verhogen van informatieveiligheid en deelname aan bewustzijnstrajecten en zien toe op deelname;
- 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 en helpt waar nodig actief mee aan het opstellen hiervan in relatie tot informatieveiligheid;
- Iedereen draagt zijn/haar toegangspas zichtbaar;
- Iedereen helpt mee om zo snel mogelijk opvolging te geven aan gemelde veiligheidsincidenten.

Organisatie

- Alle processen, systemen, data, applicaties hebben altijd minimaal 1 (proces)eigenaar; er is altijd iemand primair verantwoordelijk voor de bescherming en juist gebruik van de informatie, hij/zij bepaalt het risico op aantasting van de informatie en legt de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie vast;
- Alle informatie in systemen met DigiD-koppeling is geclassificeerd en kent een role based autorisatiemodel;
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie;
- 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 en in beeld gebracht door middel van een (pre)-DPIA en baselinetoets BIO;
- Er wordt gewerkt met DPIA's, BCP en classificatie om risicovolle processen te bepalen;
- Het inbouwen van waarborgen voor periodieke naleving van het informatieveiligheidsbeleid aan het college van burgermeester en wethouders, de gemeenteraad en eventuele toezichthouders;

- Tijdens P&C-gesprekken is aandacht voor informatieveiligheid;
- Risicovolle verwerkingen maken onderdeel uit van de auditplannen;
- Informatieveiligheid is onderdeel van elk projectplan/programma van eisen bij aanschaf of aanpassing van informatiesystemen en/of processen;
- Door middel van een Information Security Management System (ISMS/PMS) kunnen wij sturen op de kwaliteit van informatieveiligheid ;
- Dit beleid wordt ieder jaar geëvalueerd en elke 4 jaar of eerder bij een grote wijziging geactualiseerd;
- Het inbouwen van waarborgen voor periodieke naleving van het informatieveiligheidsbeleid aan het college van burgermeester en wethouders, de gemeenteraad en eventuele toezichthouders;
- Persoonsgegevens worden alleen voor een wel bepaald, uitdrukkelijk vooraf 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 waarbij altijd vooraf wordt onderzocht of het doel met minder persoonsgegevens kan worden bereikt;
- De proceseigenaar omschrijft in het 'register van verwerkingen' alle processen met persoonsgegevens per categorie en houdt dit actueel;
- Bij samenwerking met externe partijen leggen we afspraken over de informatieveiligheid vast;
- De proceseigenaar bepaalt en onderbouwt de mate van bescherming van de bedrijfsprocessen;
- Verzoeken met betrekking tot de rechten van betrokkenen op het gebied van de AVG kunnen zonder belemmeringen worden gedaan;
- Wij zijn duidelijk over wat we verwerken in onze privacyverklaring en onze formulieren;
- Iedereen helpt mee om zo snel mogelijk opvolging te geven aan gemelde veiligheidsincidenten.

Techniek

- Iedereen heeft toegang tot die informatie die ze nodig hebben voor de uitoefening van hun werk;
- De proceseigenaar controleert periodiek dat alleen geautoriseerde medewerkers de juiste persoonsgegevens inzien en verwerken en legt deze controle vast;
- Iedereen kan gebruik maken van veilig mailen volgens de NTA 7516 norm en gebruikt dit overeenkomstig gemaakte afspraken;
- Iedereen geeft actief uit zichzelf aan of er toegang is tot teveel gegevens die niet nodig zijn voor het werk of vervanging van een collega;
- Er vindt continu monitoring plaats op onze ICT infrastructuur en wordt, indien nodig, direct opgevolgd door een response unit;

- We passen basismaatregelen toe, zoals meerfactorauthenticatie (MFA), netwerksegmentatie, encryptie van de ICT infrastructuur en toetsen de werking hiervan (bijvoorbeeld door kwetsbaarheidsscans en penetratietesten).

Bijlage 2 – RASCI model

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.