gemeente doesburg

GEMEENTEBLAD

Officiële uitgave van de gemeente Doesburg

Nr. 540461

23 november 2026

Informatieveiligheidsbeleid gemeente Doesburg Strategisch informatieveiligheidsbeleid 2027 – 2029

Het college van burgemeester en wethouders van Doesburg

Besluit vast te stellen:

Informatieveiligheidsbeleid gemeente Doesburg Strategisch informatieveiligheidsbeleid 2027 – 2029

Dit besluit treedt in werking op de dag na die van de bekendmaking hiervan in het Gemeenteblad en is van toepassing op de periode van 1 januari 2027 tot 1 januari 2030.

Informatieveiligheid in één oogopslag



1. Inleiding

Inwoners, bedrijven, ketenpartners en medewerkers moeten erop kunnen vertrouwen dat de informatie die de gemeente Doesburg verwerkt betrouwbaar is en dat wij zorgvuldig met gegevens omgaan. Voor vrijwel al haar taken is de gemeente afhankelijk van informatiesystemen, gegevens en digitale voorzieningen. De veiligheid van die informatie is daarmee een voorwaarde voor betrouwbare dienstverlening en een weerbare organisatie.

Dit beleid beschrijft het strategisch informatieveiligheidsbeleid van de gemeente Doesburg voor 2027 tot en met 2029. Het vervangt het Informatieveiligheidsbeleid 2023-2026. Het beleid is geactualiseerd in verband met nieuwe relevante wetgeving en omdat ontwikkelingen zoals AI een steeds belangrijker rol spelen in onze digitale veiligheid.

De geldigheidsperiode van het beleid is in dit geval wat korter dan gebruikelijk in verband met het fusieproces waarin de gemeente zich momenteel bevindt. Deze periode dekt de maximale te verwachte tijd totdat de nieuwe gemeente een feit is.

Vanuit het perspectief van Informatieveiligheid is voorgenomen fusie met drie andere gemeenten in de Liemers een goede ontwikkeling. In de huidige organisatie zijn te weinig mensen en uren beschikbaar om alle taken die een rol spelen bij een goed beveiligde organisatie te borgen. Mensen hebben soms ook te veel rollen in de organisatie, wat tegenstrijdige belangen met zich mee kan brengen.

Het beleid is bewust compact gehouden: het beschrijft waar wij voor staan, welke kaders gelden en hoe verantwoordelijkheden zijn belegd. De operationele uitwerking staat beschreven onderliggende processen, procedures en handboeken in de betreffende afdelingen en bedrijfsonderdelen.

1.1 Wat is informatieveiligheid?

Informatieveiligheid gaat over het beschermen, beheren en beheersen van informatie, in elke vorm. Dat betreft digitale dreigingen zoals misbruik van accounts, ransomware en uitval van systemen, maar ook informatie op papier die door de verkeerde persoon wordt ingezien. Informatieveiligheid bestaat uit twee samenhangende disciplines: informatiebeveiliging en privacy.

Informatiebeveiliging richt zich op de bescherming van alle voor de organisatie relevante informatie, beoordeeld op beschikbaarheid, integriteit en vertrouwelijkheid. Privacy richt zich specifiek op het zorgvuldig en rechtmatig verwerken van persoonsgegevens en op de rechten van betrokkenen, zoals het recht op inzage. De disciplines overlappen, maar geen van beide is een onderdeel van de ander: elk borgt iets wat de ander niet borgt. Daarom beschouwen wij ze in samenhang en vatten wij ze samen onder de noemer informatieveiligheid.

1.2 Dreigingsbeeld en ontwikkelingen

Het dreigingslandschap voor gemeenten is de afgelopen jaren verbreed en geprofessionaliseerd. Voor de beleidsperiode 2027-2029 zijn de volgende ontwikkelingen leidend voor de inzet:

- Ransomware en afpersing blijven een reëel risico, met directe gevolgen voor de continuïteit van de dienstverlening aan inwoners.
- Aanvallen via de keten en via leveranciers nemen toe. Een kwetsbaarheid bij een leverancier of ketenpartner raakt direct de gemeente.
- Kunstmatige intelligentie verandert zowel de aanval als de verdediging. Aanvallers zetten AI in voor overtuigende phishing, deepfakes en geautomatiseerde aanvallen. Tegelijk biedt AI kansen voor detectie en respons.
- De toenemende digitalisering, cloudgebruik en ketensamenwerking vergroten het aanvalsoppervlak en de afhankelijkheid van derden.
- Het wettelijk kader wordt strenger. De Cyberbeveiligingswet stelt expliciete eisen aan beheersing, melding en bestuurlijke verantwoordelijkheid.

Deze ontwikkelingen bepalen waar de organisatie de komende jaren aan moet werken. Ze keren terug in de ambities, kaders en uitgangspunten in hoofdstuk 2.

1.3 Doel en scope

Dit beleid biedt richting aan bestuur, management en medewerkers bij het maken van afwegingen over risico's, maatregelen en verantwoordelijkheden. Het vormt de kapstok voor onderliggende veiligheidsplannen en documenten.

De scope omvat:

- Alle gemeentelijke processen en de onderliggende informatiesystemen, applicaties, infrastructuur, voorzieningen en gegevensverzamelingen;

- Alle informatie-uitwisseling met externe partijen, waaronder verbonden partijen, leveranciers en ketenpartners;
- Het gebruik van informatie door medewerkers, bestuurders, ingehuurde krachten en ketenpartners, ongeacht locatie, tijdstip en gebruikte apparatuur;
- Cloud-, platform- en SaaS-diensten;
- Objecten, procesautomatisering en operationele technologie voor zover deze raken aan de gemeentelijke taakuitvoering;
- Internetdomeinen en aan de gemeente gekoppelde digitale toegangen die van belang zijn voor bereikbaarheid, dienstverlening, continuïteit en herkenbaarheid.

Voor een aantal vakgebieden gelden aanvullende, wettelijk voorgeschreven beveiligingseisen die in afzonderlijke documenten zijn uitgewerkt, waaronder BRP, DigiD, Suwinet, BAG, BGT, BRO en WOZ. (Zie verklaring afkortingen in bijlage 2)

2. Strategisch beleid

Dit hoofdstuk beschrijft de kern van het beleid: onze ambitie, de doelen, de geldende kaders en de uitgangspunten waaraan iedereen binnen de organisatie zich houdt.

2.1 Ambitie

De gemeente Doesburg wil een digitaal weerbare organisatie zijn die haar dienstverlening ook onder druk kan voortzetten en die zorgvuldig met gegevens omgaat. Voor 2027-2029 streven wij de volgende ambities na:

- Wij groeien in volwassenheid en verschuiven geleidelijk van ‘het voldoen aan wettelijke normen’ naar een situatie waarin we ook kunnen aantonen dat beveiligingsmaatregelen goed werken in onze organisatie.
- De mens wordt onze eerste verdedigingslinie, in alle lagen van de organisatie en op bestuurlijk niveau.
- Wij kunnen incidenten snel detecteren, beheersen en ervan leren, en wij borgen de continuïteit van de kritieke processen.
- Wij hanteren de principes ‘beveiliging en privacy by design’ als vertrekpunt bij nieuwe initiatieven, wijzigingen en aanbestedingen.
- Wij gaan beheerst en verantwoord om met cloudgebruik, digitale autonomie en leveranciersafhankelijkheid.
- Wij gaan beheerst en verantwoord om met algoritmen en kunstmatige intelligentie, met aandacht voor zowel de kansen als de dreigingen.

2.2 Doelen

Aansluitend op de landelijke handreiking van de Informatiebeveiligingsdienst hanteren wij drie hoofddoelen:

1. Risico's beheersen en incidenten voorkomen. Wij brengen risico's onderbouwd in beeld en treffen passende maatregelen om de kans op en de impact van incidenten te beperken.
2. De veiligheid van bedrijfsmiddelen en persoonsgegevens waarborgen. Wij beschermen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en verwerken persoonsgegevens rechtmatig, behoorlijk en transparant.
3. Naleving en reactievermogen verbeteren. Wij voldoen aantoonbaar aan wet- en regelgeving en normenkaders en zijn in staat om adequaat te reageren op incidenten en verstoringen.

2.3 Wettelijk en normatief kader

Dit beleid is opgesteld op basis van geldende wet- en regelgeving en verplichte normenkaders.

2.3.1 Informatiebeveiliging: BIO2 en ISO

De Baseline Informatiebeveiliging Overheid 2 (BIO2) is het verplichte kader voor informatiebeveiliging binnen de overheid. De BIO2 is gebaseerd op het beheersen van risico's en sluit aan op de internationale kwaliteitsnormen ISO 27001 en ISO 27002.
De gemeente werkt met een managementsysteem voor informatiebeveiliging (ISMS).
Hierbij wordt gewerkt volgens een vaste verbetercyclus van plannen, uitvoeren, controleren en bijsturen. Deze cyclus sluit aan op de reguliere planning- en controlcyclus van de gemeente.

2.3.2 Cyberbeveiligingswet

De Cyberbeveiligingswet is de Nederlandse uitwerking van de Europese NIS2-richtlijn en vervangt de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze wet is op 15 augustus 2026 in werking getreden en is gedurende deze beleidsperiode bepalend voor de inrichting van onze informatieveiligheid. Voor de sector overheid wordt de zorgplicht ingevuld op basis van de BIO2. De BIO2 vormt daarmee tegelijk ons normenkader en de wettelijke ondergrens. De wet kent voor de organisatie de volgende kernverplichtingen:

- Zorgplicht: het nemen van passende en evenredige technische, operationele en organisatorische maatregelen om risico's te beheersen, onderbouwd met een risicoanalyse en aantoonbare implementatie.
- Meldplicht: het melden van significante incidenten bij de bevoegde instantie, met een eerste melding binnen 24 uur en een uitgebreidere melding binnen 72 uur.
- Registratieplicht: het aanmelden van de organisatie bij de daarvoor aangewezen instantie, waarmee toegang ontstaat tot dreigingsinformatie en ondersteuning.

De wet legt nadrukkelijk een verantwoordelijkheid bij de bestuurlijke en ambtelijke top. Bestuurders en managers zijn verantwoordelijk voor het goedkeuren van de maatregelen en het toezicht daarop, en kunnen hierop persoonlijk worden aangesproken. Op de naleving wordt onafhankelijk toezicht gehouden. Dit beleid, het ISMS en de bestuurlijke verantwoordingslijnen zijn zo ingericht dat de gemeente aan deze verplichtingen kan voldoen en dit aantoonbaar kan maken.

2.3.3 Privacy: AVG, UAVG en Wpg

Voor de bescherming van persoonsgegevens volgen wij de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de Wet politiegegevens (Wpg), met de daaraan gerelateerde regelgeving. Wij verwerken persoonsgegevens alleen voor een welbepaald, gerechtvaardigd doel en op basis van een grondslag, en bewaren deze gegevens niet langer dan nodig.

2.3.4 Algoritmen en kunstmatige intelligentie

Kunstmatige intelligentie raakt informatieveiligheid op twee manieren en krijgt daarom in deze beleidsperiode expliciet aandacht.

Als toepassing: bij de inzet van algoritmen en AI houden wij rekening met de toepasselijke Europese en nationale kaders, waaronder de AI Act, en met regels voor rechtmatigheid, transparantie, menselijk toezicht, beveiliging en grondrechten. Toepassingen worden vooraf beoordeeld op risico's, onder meer via een AI- of algoritme-assessment en, waar persoonsgegevens worden verwerkt, een DPIA. Risicovolle algoritmen worden opgenomen in het algoritmeregister. Medewerkers gebruiken AI-toepassingen uitsluitend voor legitieme werkdoeleinden en volgens de geldende afspraken.

Als dreiging: aanvallers zetten AI in voor steeds overtuigender phishing, voor deepfakes die gericht zijn op misleiding en fraude, en voor het opschalen en versnellen van aanvallen. Wij houden hier rekening mee in onze bewustwording, detectie en respons, en passen onze werkwijze en processen aan naarmate deze dreiging zich ontwikkelt. De governance van AI is onlosmakelijk verbonden met informatiebeveiliging en privacy en wordt in dat verband beschouwd.

2.3.5 Overige kaders

Wij houden rekening met andere relevante wet- en regelgeving en gemeentelijke kaders en passen deze toe waar nodig. Denk hierbij b.v. aan regelgeving op gebied van digitale dienstverlening, archivering, continuïteit, inkoop, cloudgebruik en digitale autonomie.

2.4 Uitgangspunten: mens, organisatie en techniek

Informatieveiligheid is meer dan techniek en is niet alleen een zaak van ICT. Door het te benaderen vanuit de drie samenhangende invalshoeken mens, organisatie en techniek, krijgt het de noodzakelijke aandacht in de volle breedte van de organisatie. De volgende uitgangspunten gelden voor iedereen. De concrete invulling staat in bijlage 1 en wordt uitgewerkt in het Informatieveiligheidsplan en de onderliggende procedures.

Mens

- Iedereen draagt actief bij aan de bewustwording rond informatieveiligheid.
- Iedereen beschermt gegevens tegen ongeautoriseerde toegang, gebruik, wijziging, openbaarmaking, vernietiging, verlies of overdracht.
- Iedereen meldt een veiligheidsincident, kwetsbaarheid of vermoeden van een datalek onmiddellijk volgens de geldende procedure.
- Werkplekken, schermen en documenten worden zo achtergelaten dat onbevoegde kennisneming wordt voorkomen.
- Medewerkers gebruiken informatie, systemen en AI-toepassingen zorgvuldig en uitsluitend voor legitieme werkdoeleinden.

Organisatie

- Het college is eindverantwoordelijk en stelt de benodigde mensen en middelen beschikbaar.
- Via een DVO met de gemeente Doetinchem nemen we ICT Diensten af bij ICT Samen. Deze serviceorganisatie is verantwoordelijk voor levering en onderhoud van onze ICT infrastructuur, onze digitale werkplekken en de werkapparatuur.

- Onze gemeentesecretaris maakt onderdeel uit van het directieteam (GS overleg) dat op strategisch niveau beslissingen neemt over deze serviceorganisatie.
- Managers en teamleiders zijn integraal verantwoordelijk voor informatieveiligheid binnen hun domein/afdeling en bevorderen actief kennis en bewustzijn.
- Informatieveiligheid is integraal onderdeel van het risicomanagement; risico's worden vooraf afgewogen bij nieuwe initiatieven, wijzigingen, cloudmigraties en samenwerkingen.
- Kritieke bedrijfsprocessen worden onderbouwd bepaald en beschermd; informatieveiligheid, privacy, bedrijfscontinuïteit en crisisbeheersing worden in samenhang beschouwd, in lijn met een bedrijfscontinuïteitsplan (BCP) en de opschaalorganisatie cybercrisis.
- Wij stellen aan leveranciers, ketenpartners en verbonden partijen eisen die passen bij de risico's van de dienstverlening, en houden rekening met continuïteit, auditmogelijkheden, exitstrategie en ongewenste afhankelijkheden.
- Voor internetdomeinen en digitale toegangen die van belang zijn voor de dienstverlening borgen wij eigenaarschap, registratie, beheer en verlenging.
- Informatieveiligheid is een continu verbeterproces.

Techniek
- Informatiesystemen worden ingericht en beheerd conform standaarden en voldoen aan wet- en regelgeving.
- Wij beheersen de toegang tot informatiesystemen om ongeautoriseerde toegang te voorkomen.
- Logging, back-up, herstel, patching, monitoring en kwetsbaarhedenbeheer worden passend ingericht en de werking wordt getoetst, onder meer via kwetsbaarheidsscans en penetratietesten.
- Procesautomatisering, objecten en gekoppelde digitale voorzieningen worden expliciet meegenomen in de beveiligingsaanpak.
- Cloud- en platformdiensten worden alleen toegepast bij aantoonbaar passende beheersing van beveiliging, privacy, continuïteit en exitstrategie.

2.5 Uitvoering en middelen
Dit beleid wordt jaarlijks getoetst d.m.v. audits en rapportages die uitmonden in een Informatieveiligheidsplan, dat de concrete acties, planning en evt. extra benodigde capaciteit beschrijft. Waar de uitvoering aanvullende mensen of middelen vraagt, wordt dit in het Informatieveiligheidsplan inzichtelijk gemaakt en langs de planning- en controlcyclus en de begroting belegd. Het college stelt de benodigde mensen en middelen beschikbaar en doet daarvoor waar nodig een voorstel aan de gemeenteraad.

3. Organisatie, taken en verantwoordelijkheden

Informatieveiligheid is niet alleen een zaak van ICT of van enkele specialisten. Het college, de gemeentesecretaris, managers, teamleiders en medewerkers spelen elk een rol. Het management weegt het belang van informatie, de risico's en de te treffen of te accepteren maatregelen. De toewijzing van verantwoordelijkheden voor ketens, privacy, procesautomatisering, continuïteit en objecten ligt in de lijn.

De rollen zijn ingedeeld volgens de RASCI-methodiek: Responsible (verantwoordelijk voor de uitvoering), Accountable (eindverantwoordelijk), Supportive (ondersteunend), Consulted (geraadpleegd en adviserend) en Informed (geïnformeerd).

Deze verdeling sluit aan op het Three Lines Model. De lijn vormt de eerste lijn en is verantwoordelijk voor de uitvoering en de beheersing. De CISO en de FG vormen de tweede lijn en adviseren en toetsen onafhankelijk. De externe auditor vervult de derde lijn met onafhankelijke assurance, onder meer in het kader van ENSIA.

3.1 Rollen
Eindverantwoordelijk (Accountable)
Het college van burgemeester en wethouders is eindverantwoordelijk voor de informatieveiligheid, stelt dit beleid vast en doet voor de benodigde middelen een voorstel aan de gemeenteraad. Onder de Cyberbeveiligingswet keuren het college en de gemeentesecretaris als bestuurlijke en ambtelijke top de maatregelen goed en houden zij daarop toezicht; zij kunnen hierop persoonlijk worden aangesproken.

Verantwoordelijk (Responsible)
De gemeentesecretaris/algemeen directeur zorgt dat de portefeuillehouder gevraagd en ongevraagd worden geïnformeerd over het niveau van informatieveiligheid, en wordt daarover geïnformeerd door de CISO, de FG en de managers. De gemeentesecretaris stelt het jaarlijkse Informatieveiligheidsplan en evt. onderliggende documenten vast, voor zover die bevoegdheid niet elders is belegd.

Managers zijn integraal verantwoordelijk voor de uitvoering van dit beleid binnen hun afdeling en leggen daarover verantwoording af aan de gemeentesecretaris. Managers dragen het beleid en de

bijbehorende procedures uit binnen hun teams. Medewerkers zijn zelf verantwoordelijk voor het veilig gebruik van apparatuur en informatie en voor het volgen van de geldende afspraken.

Adviserend en toetsend (Consulted)
De CISO heeft een onafhankelijke positie ten opzichte van het management en het college. De CISO adviseert gevraagd en ongevraagd over informatieveiligheid op basis van risicogestuurd werken, toetst de opzet en werking van maatregelen, en rapporteert hierover rechtstreeks aan de gemeentesecretaris. De CISO heeft een directe escalatielijn naar de gemeentesecretaris wanneer de informatieveiligheid in het geding komt. Deze adviserende en toetsende rol laat de verantwoordelijkheid en het eigenaarschap in de lijn onverlet: de CISO is niet de eigenaar van de maatregelen, maar bewaakt, adviseert, toetst en escaleert.

De FG heeft eveneens een onafhankelijke positie, adviseert gevraagd en ongevraagd over privacy, houdt toezicht op de naleving van de privacywetgeving en heeft een directe escalatielijn naar de gemeentesecretaris. De FG rapporteert jaarlijks aan het college over de naleving van de privacywetgeving.

Ondersteunend (Supportive)
De informatieveiligheidscoördinatoren (IVC) ondersteunen de organisatie op tactisch en operationeel niveau met onder meer de coördinatie van ENSIA, toetsingen, DPIA's en registers, en de voortgangsrapportage. Voorbeelden van deze rol zijn de Privacy Officer (PO), Information Security Officer (ISO). Op specifieke deelgebieden geldt soms een voorgeschreven benaming, zoals, beveiligingsfunctionaris BRP, beveiligingsfunctionaris reisdocumenten en security officer Suwinet.
De informatieveiligheidsbeheerders (IVB), vaak ingevuld door de functioneel applicatiebeheerder, voeren op operationeel niveau de maatregelen uit en signaleren incidenten binnen hun applicatie en processen. Daarnaast vervult de organisatie de rollen van contactpersoon richting de Informatiebeveiligingsdienst (IBD) en het Nationaal Cyber Security Centrum (NCSC).

Te informeren (Informed)
De gemeenteraad bepaalt op hoofdlijnen het beleid, beslist over de middelen in de begroting en houdt toezicht op de uitvoerig en heeft daarmee ook een bestuurlijke verantwoordelijkheid voor de mogelijkheden voor de uitvoering van dit beleidsplan. Concern control richt zich op de planning- en controlcyclus en heeft een rol in de doorontwikkeling van risicomanagement en verantwoording.

3.2 Risicoacceptatie
Honderd procent veiligheid bestaat niet, er blijven altijd restrisico's, ook na het nemen van uitgebreide veiligheidsmaatregelen. Uitgangspunt is dat de proceseigenaar in de lijn het restrisico accepteert en dat zwaardere restrisico's worden geëscaleerd naar het niveau dat daarover kan besluiten.

4. Samenwerking

De gemeente staat er niet alleen voor. Regionaal en landelijk werken wij samen om kennis en krachten te bundelen en de informatieveiligheid te vergroten.

4.1 Regionaal
Op het gebied van ICT werkt de gemeente Doesburg samen met omliggende gemeenten en organisaties binnen de Achterhoek, met de gemeente Doetinchem als gastheer in het samenwerkingsverband ICT Samen. Op het gebied van informatieveiligheid stemmen de CISO's, FG's en de veiligheidscoördinatoren van de aangesloten organisaties af in vaste overlegstructuren, gericht op kennisdeling, gezamenlijke verkenning en het beheersen en verbeteren van de beveiliging van de samenwerking. In verband met de mogelijk aankomende fusie met de Liemerse gemeenten zal de komende jaren ook de samenwerking met deze gemeenten en het contact met die CISO's en de FG's een steeds grotere rol gaan spelen.

4.2 Landelijk
De gemeente maakt gebruik van landelijke ondersteuning. Deze partijen zijn concreet van belang voor:
- Nationaal Cyber Security Centrum (NCSC): de sectorale CERT/CSIRT voor gemeenten. de nationale instantie voor dreigingsinformatie, analyse en advies, en inmiddels ook het wettelijk meldpunt onder de Cyberbeveiligingswet.
- Informatiebeveiligingsdienst (IBD): Expertisecentrum voor gemeente op informatiebeveiliging, deelt dreigingsinformatie en kennis op gebied van informatiebeveiliging en privacy.
- VNG Realisatie: ontwikkelt gezamenlijke gemeentelijke oplossingen, standaarden en handreikingen die wij, waar passend, toepassen in onze gemeente.
- Centrum Informatiebeveiliging en Privacybescherming (CIP): een publiek-private netwerkorganisatie die kennis en producten levert voor informatieveiligheid in ketens.

4.3 Leveranciers, ketenpartners en verbonden partijen

De gemeente maakt voor haar dienstverlening gebruik van leveranciers, cloudpartijen, ketenpartners en verbonden partijen. Bij uitbesteding blijft de gemeente verantwoordelijk voor passende sturing, toezicht en verantwoording. Daarom stellen wij waar nodig eisen aan informatiebeveiliging, privacy, auditrechten, incidentmelding, continuïteit, logging, exitstrategie, dataportabiliteit en de beheersing van afhankelijkheden. Wij sluiten aan op de gemeentelijke inkoopvoorwaarden en maken de afspraken passend bij de aard van de dienstverlening en de risico's van de verwerking of systeemafhankelijkheid.

5. Controle en verantwoording

De gemeente stuurt en verantwoordt via een samenhangende cyclus van het Informatieveiligheidsplan, de CISO-rapportage, de FG-rapportage en de ENSIA-verantwoording. Er wordt gewerkt volgens een plan-do-check-act-cyclus die aansluit op de planning- en controlcyclus van de gemeente. Bevindingen uit audits, toetsingen, incidenten, datalekken en risicoanalyses vormen de input voor verbetermaatregelen in het Informatieveiligheidsplan.

5.1 ENSIA en collegeverklaring

Het college verantwoordt zich jaarlijks over informatiebeveiliging via de ENSIA-zelfevaluatie. Op basis van de uitkomsten stelt het college een collegeverklaring op waarin het aangeeft in hoeverre de gemeente voldoet aan de relevante normenkaders. Waar vereist ondersteunt een onafhankelijke externe IT-auditor deze verantwoording met assurance of een afzonderlijke controle. Het college rapporteert de uitkomsten aan de gemeenteraad. De ISO coördineert de totstandkoming van de zelfevaluatie en de collegeverklaring inhoudelijk, met ondersteuning van de CISO, en Functioneel Applicatiebeheers.

5.2 Informatiebeveiliging

De CISO rapporteert jaarlijks over de uitvoering en naleving van het beleid aan het MT en de gemeentesecretaris en, waar nodig, aan de portefeuillehouder. De CISO-rapportages geven inzicht in risico's, voortgang maatregelen, incidenten en relevante ontwikkelingen.

5.3 Privacy

De FG rapporteert jaarlijks schriftelijk en rechtstreeks aan het college over de mate waarin de organisatie de privacywetgeving naleeft. De rapportage maakt duidelijk op welke onderwerpen wordt voldaan en waar verbetering nodig is, met aanbevelingen en prioriteiten.

5.4 Aanvullende audits

Voor specifieke domeinen worden aanvullende interne of externe audits uitgevoerd.
Zo wordt er bijvoorbeeld jaarlijks een zelfaudit uitgevoerd op de veiligheid van de BRP. Hierop kan een mogelijke steekproef van het ministerie plaatsvinden. De uitkomsten worden gebruikt om de organisatie verder te verbeteren.

5.5 Inbedding en evaluatie

Informatieveiligheid is ingebed in de PDCA-cyclus, zodat risico's, afwijkingen en voortgang periodiek in beeld komen, onder meer in de P&C-gesprekken. De gemeente hanteert een ISMS en waar passend aanvullende registratiesystemen om de kwaliteit te monitoren en te verbeteren.

Dit beleid geldt voor de periode 2027 tot en met 2029 of korter, in het geval Doesburg eerder onderdeel gaat worden van de fusiegemeente de Liemers. Het beleid wordt aan het einde van de looptijd geëvalueerd en tussentijds aangepast als ontwikkelingen in wetgeving, dreiging, techniek of organisatie daartoe aanleiding geven.

Aldus vastgesteld door het college op 10 november 2026

De secretaris
Peter Werkman

de burgemeester
Rob Bats

Bijlage 1: Concrete invulling van de uitgangspunten

Deze bijlage maakt de uitgangspunten uit paragraaf 2.4 concreet. Het is de praktische vertaling naar wat de uitgangspunten in de dagelijkse uitvoering betekenen.

Mens
- Nieuwe medewerkers en bestuurders krijgen bewustwording over informatieveiligheid als onderdeel van hun inwerkprogramma aangeboden.
- Iedereen neemt actief deel aan het doorlopende bewustzijnsprogramma van de gemeente.
- Managers stimuleren deelname aan het bewustzijnsprogramma en zien daarop toe.
- Iedereen kent de voor de eigen functie relevante beleidsdocumenten en werkinstructies en handelt daarna.
- Medewerkers worden gestimuleerd om veiligheidsincidenten te melden

Organisatie
- Alle processen, systemen, data en applicaties hebben een eigenaar die primair verantwoordelijk is voor de bescherming en het juiste gebruik.
- De proceseigenaar bepaalt en onderbouwt de mate van bescherming en is integraal verantwoordelijk voor de uitvoering, inclusief de ketens van informatiesystemen.
- Maatregelen worden bepaald in relatie tot het risico, in beeld gebracht via risicoanalyses, DPIA's en toetsingen, er wordt gewerkt met classificatie en continuïteitsafwegingen.
- Informatieveiligheid is onderdeel van elk projectplan en van het programma van eisen bij aanschaf of aanpassing van systemen en processen.
- Risicovolle verwerkingen en kritieke processen maken onderdeel uit van auditplannen en verbeteracties;
- Tijdens P&C-gesprekken is er aandacht voor informatieveiligheid.
- Persoonsgegevens worden alleen voor een welbepaald, gerechtvaardigd doel en op basis van een grondslag verwerkt, en niet langer bewaard dan nodig; afspraken met externe partijen worden vastgelegd.
- Voor internetdomeinen en digitale toegangen worden eigenaarschap, registratie, beheer, verlenging en overdraagbaarheid geborgd.

Techniek
- Iedereen heeft alleen toegang tot de informatie die nodig is voor het werk;
- de proceseigenaar controleert periodiek de autorisaties en legt dit vast.
- Veilig mailen wordt toegepast volgens de geldende afspraken.
- Er vindt passende monitoring plaats op de ICT-infrastructuur, met directe opvolging waar nodig.
- Basismaatregelen zoals meervoudige authenticatie, netwerksegmentatie en encryptie worden toegepast en de werking wordt getoetst.
- Er wordt gewerkt met centraal beheerde en beveiligde apparatuur

Bijlage 2: Verklaring gebruikte afkortingen

- **BRP – Basisregistratie Personen**
  Registratie met persoonsgegevens van inwoners en niet-ingezetenen, beheerd door gemeenten.
- **DigiD – Digitale Identiteit**
  Het officiële inlogsysteem waarmee burgers zich digitaal identificeren bij overheidsorganisaties.
- **Suwinet - Structuur Uitvoeringsorganisatie Werk en Inkomen**
  Elektronische infrastructuur waarmee gemeenten, UWV en SVB gegevens uitwisselen voor hun wettelijke taken.
- **BAG – Basisregistratie Adressen en Gebouwen**
  Landelijke registratie van adressen en gebouwen in Nederland.
- **BGT – Basisregistratie Grootschalige Topografie**
  De gedetailleerde digitale basiskaart van Nederland met gebouwen, wegen, water, groen en spoorlijnen.
- **BRO – Basisregistratie Ondergrond**
  Bevat gegevens over de geologische en bodemkundige opbouw van de ondergrond, grondwater en bodemonderzoeken.
- **WOZ – Waardering Onroerende Zaken**
  Wettelijk systeem voor het vaststellen van de waarde van woningen en andere onroerende zaken.