Gemeente Maastricht

# GEMEENTEBLAD

Officiële uitgave van de gemeente Maastricht

Nr. 26265

22 januari

2026

## Strategisch informatiebeveiligingsbeleid versie 3.0

Gezien het voorstel van burgemeester en wethouders d.d. 16 december 2025, registratienummer 2025 04438;

Besluit:

1. Vaststellen van het Strategisch informatiebeveiligingsbeleid versie 3.0.
2. Intrekken van het op 8 november 2022 door het college van B&W van de gemeente Maastricht vastgestelde strategisch informatiebeveiligingsbeleid versie 2.0.

### Inleiding

Dit document beschrijft het strategische informatiebeveiligingsbeleid van de gemeente Maastricht voor de periode 2025-2028 en vervangt het in 2022 vastgestelde `Informatiebeveiligingsbeleid gemeente Maastricht'. Het voorgaande beleid was gebaseerd op de gemeentelijke Visie op Informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO) versie 1.04zv en de 10 bestuurlijke principes voor informatiebeveiliging.

De basis voor dit strategisch beleid is de NIS2 richtlijn, de Cyberbeveiligingswet waarin de verplichtingen die de NIS2 richtlijn oplegt, onverkort zijn overgenomen, de NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 normatiek en de daarvan afgeleide Baseline Informatiebeveiliging Overheid 2 (BIO2).

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

### Informatiebeveiliging

Onder informatiebeveiliging[1] verstaat de gemeente Maastricht: “het treffen en onderhouden van een samenhangend pakket van preventieve, detectieve, repressieve en correctieve maatregelen, om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van alle gemeentelijke informatie ongeacht de vorm en inhoud.

Informatiebeveiliging gaat niet over ICT alleen, maar gaat over informatie in alle verschijningvormen binnen de organisatie, inclusief Operationele Technologie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

Informatiebeveiliging creëert daarmee waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de gemeentelijke organisatie.

### Visie Informatiebeveiliging

De gemeente Maastricht kijkt naar Informatieveiligheid vanuit de volgende 6 gezichtspunten:

1. Betrouwbaarheid: De gemeente is een betrouwbare organisatie, die zorgvuldig omgaat met (bijzondere) persoonsgegevens van burgers en medewerkers.
2. Bewustwording: De gemeentelijke organisatie borgt het bewustzijn inzake veilige omgang met gegevens bij alle medewerkers; immers het passend beveiligen van informatie is een taak voor ons allemaal.
3. Wet- en regelgeving: De gemeente voldoet aan de geldende (bijzondere) wet- en regelgeving op het gebied van Informatiebeveiliging.
4. Risicomanagement: Risico’s met betrekking tot informatiebeveiliging worden afgewogen, daarmee wordt het onbewust lopen van risico’s omgebogen in bewust aanvaardbare risico’s nemen. 100% beveiliging is immers niet mogelijk.

1) Betreft het taakveld informatieveiligheid (het wat) en informatiebeveiliging (het hoe).

5. Techniek en organisatie: De gemeente neemt passende technische en organisatorische maatregelen om het verwerken en beheren en reconstrueren van informatie te beveiligen. Incidenten gaan komen en daar is voorbereiding voor nodig.
6. Fysieke veiligheid: De gemeente zorgt voor afdoende fysieke beveiliging van gebouwen, medewerkers en informatie.

## Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het Strategisch Informatiebeveiligingsbeleid zijn de volgende:

### NIS2

De Europese NIS2-richtlijn is sinds 17 oktober 2024 van kracht. De richtlijn legt aan essentiële entiteiten, waaronder gemeentelijke overheden, een zorg-, meld- en toezichtplicht op.

Zorgplicht – Deze verplicht organisaties zelf een risicobeoordeling uit te voeren. Op basis van deze risicobeoordeling nemen zij passende maatregelen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.

Meldplicht – De richtlijn schrijft voor dat entiteiten incidenten binnen 24 uur moeten melden bij de toezichthouder. Het gaat om incidenten die de continuïteit van dienstverlening van de essentiële entiteit aanzienlijk (kunnen) verstoren. In het geval van een cyberincident moet het ook gemeld worden bij het Computer Security Incident Response Team (CSIRT). Voor gemeenten is de Informatie Beveiliging Dienst (IBD) het Computer Security Incident Response Team.

Toezichtplicht – Organisaties die onder de richtlijn vallen, krijgen ook verplicht toezicht. De NIS2-richtlijn schrijft voor dat een onafhankelijk toezichthouder kijkt naar de naleving van de verplichtingen uit de richtlijn. Voor de overheid wordt de Rijksinspectie Digitale Infrastructuur (RDI) aangewezen als toezichthouder. De RDI maakt voor het toezicht op NIS2 voor de overheid gebruik van bestaande verantwoordingsstructuren, waaronder ENSIA.

### Cyberbeveiligingswet

In 2026 treedt de Cyberbeveiligingswet in werking. Deze wet wordt de Nederlandse vertaling van de Network and Information Security 2 richtlijn (NIS2) van de Europese Unie.

### Baseline Informatiebeveiliging Overheid

De Cyberbeveiligingswet geeft de Baseline Informatiebeveiliging Overheid 2 als het vigerende normenkader voor de overheid. De BIO conformeert aan de internationale normen voor informatiebeveiliging, zijnde de NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 plus aanvullende maatregelen.

### Nationale Digitaliseringsstrategie

De nationale digitaliseringsstrategie die op 4 juli 2025 is gepubliceerd, kent 6 prioriteiten. Eén van deze prioriteiten raakt informatiebeveiliging en luidt:
Digitale weerbaarheid en digitale autonomie van de overheid versterken.
“We voeren een overheidsbrede aanpak voor digitale weerbaarheid en autonomie, verbeteren continu onze digitale weerbaarheid voor snel herstel bij crises, en implementeren een quantumveilige cryptografie-aanpak om risico's te beheersen”. De gemeente Maastricht sluit aan bij de overheidsbrede aanpak.

### 10 Bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging zijn opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) in samenwerking met de Informatiebeveiligingsdienst (IBD). Ze vormen een onderdeel van de Baseline Informatiebeveiliging Overheid (BIO), die sinds 2020 geldt als norm voor informatiebeveiliging binnen de Nederlandse overheid.
Zij gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur;
2. Informatiebeveiliging is van iedereen;
3. Informatiebeveiliging is risicomanagement;
4. Risicomanagement is onderdeel van de besluitvorming;
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. Informatiebeveiliging is een proces;
7. Informatiebeveiliging kost geld;
8. Onzekerheid dient te worden ingecalculeerd;
9. Verbetering komt voort uit leren en ervaring;

10. Het bestuur controleert en evalueert.

### Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten laat zien dat gemeenten in 2025-2026 staan voor een onverminderd complex digitaal dreigingslandschap. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van financiële en personele krapte.

### Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem, waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van beleid.

### Het strategisch informatiebeveiligingsbeleid van de gemeente Maastricht

**Het strategisch informatiebeveiligingsbeleid van de gemeente Maastricht conformeert aan de NIS2, de Cyberbeveiligingswet, de geldende versie van de Baseline Informatiebeveiliging Overheid, de Nederlandse digitaliseringsstrategie, de gemeentelijke Visie op Informatiebeveiliging en de 10 bestuurlijke principes voor informatiebeveiliging.**

### Scope strategisch informatiebeveiligingsbeleid

Dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen (zowel on-premise als in SaaS), procesautomatisering (OT), Artificial Intelligence, informatie en gegevens van de gemeente en van externe partijen, het gebruik daarvan door medewerkers en (keten)partners, in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur of medium.

Het strategisch informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen (bijvoorbeeld DigiD, Suwinet, gemeentelijke basisregistraties w.o. de BRP/ PUN, de verplichte standaarden van het Forum Standaardisatie etc.).
Het strategisch informatiebeveiligingsbeleid wordt, waar van toepassing, per BIO-onderwerp door het Directieteam (DT) aangevuld met tactisch beleid op voorstel van de CISO.
Manager Team Informatievoorziening & automatisering zorgt voor de doorvertaling op operationeel niveau.

### Strategische doelen

De doelen van het strategisch informatiebeveiligingsbeleid zijn:
- Het voldoen aan wet- en regelgeving.
- Het waarborgen van de continuïteit van de bedrijfsvoering.
- Het managen van de informatiebeveiliging.
- De adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorziening.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

### Randvoorwaarden

- De informatiebeveiliging en privacy-eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/ gecontroleerd.
- Kennis over en bewustzijn van informatiebeveiliging onder medewerkers en het omgaan met persoonsgegevens worden actief bevorderd en geborgd door het lijnmanagement in een doorlopende bewustwordingscampagne geïnitieerd door de Chief Information Security Officer (CISO).
- Het Bedrijfsvoeringsportfolio van uit te voeren projecten, bevat een Informatiebeveiligingsopgave. De inhoud van deze opgave wordt bepaald aan de hand van:

  - Een GAP-analyse op basis van de vigerende normenkaders en informatie uit het information security management system (ISMS);
  - Bevindingen naar aanleiding van de jaarlijkse ENSIA[2]-audit;
  - Het actuele dreigingsbeeld gemeenten[3];
  - Aandachtspunten ten aanzien van informatiebeveiliging afkomstig van de Lijnmanagers binnen de processen waarvoor zij verantwoordelijk zijn.

- Het beleid wordt gepubliceerd op de gemeentelijke website, het gemeentelijke intranet en bekendgemaakt aan nieuwe medewerkers bij in diensttreding.

## Informatiebeveiligingsorganisatie: taken en verantwoordelijkheden

Binnen de gemeente Maastricht zijn de volgende rollen met de daarbij behorende taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging benoemd en belegd:

Het **College van Burgemeester en Wethouders** is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Het college van B&W stelt het strategisch informatiebeveiligingsbeleid vast; verantwoordt zich over informatiebeveiliging aan de gemeenteraad (horizontale verantwoording) en aan de nationale toezichthouders (verticale verantwoording). Het college laat zich daarbij adviseren door een Chief Information Security Officer (CISO).

Het **Directieteam** stelt het tactisch informatiebeveiligingsbeleid vast en neemt twee keer per jaar kennis van de voortgang van de informatiebeveiligingsopgaven.

Het **Managementteam Domein Bedrijfsvoering en Dienstverlening (MT DBD)** stelt in de rol van Portfolio Stuurgroep het bedrijfsvoeringsportfolio van uit te voeren projecten vast, inclusief de Informatiebeveiligingsopgave.

**Chief Information Security Officer (CISO)**
De gemeentelijke CISO heeft een onafhankelijke positie.

De CISO is bevoegd en verantwoordelijk voor:
- Opstellen, operationaliseren en actualiseren van het samenhangend informatiebeveiligingsbeleid en zorgdragen voor daaruit voortvloeiende maatregelen (technisch en organisatorisch). Fungeren als informatiebeveiligingsadviseur. Leiden van projecten om de kwaliteit van beveiliging in de organisatie te verhogen en stimuleren van beveiligingsbewustzijn.
- Zorgdragen voor toezicht op de naleving van het informatiebeveiligingsbeleid. Initiëren en laten uitvoeren van periodieke audits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses en het doen van onderzoek. Verrichten van evaluaties en doen van verbetervoorstellen. Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten.
- Rechtstreeks rapporteren aan directie over het gevoerde beleid, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, resultaten van onderzoeken en controles op het gebied van informatiebeveiliging en onafhankelijk kunnen rapporteren aan het bestuur. Optreden als gemeentelijke coördinator ENSIA.
- Het agenderen van een informatiebeveiligingsopgave voor het bedrijfsvoeringsportfolio.

**Management lijnorganisatie**
- Is verantwoordelijk voor de uitvoering van de informatiebeveiliging. Alle informatiebronnen en -systemen die gebruikt worden door de lijn hebben een interne eigenaar. De primaire verantwoordelijkheid voor de bescherming van informatie ligt bij de eigenaar van de informatie en onderliggende data.
- Is verantwoordelijk voor de (keten)processen die onder hun verantwoordelijkheid vallen inclusief informatiebeveiliging en voor de bevordering en borging van het bewustzijn ten aanzien van informatiebeveiliging bij medewerkers.
- Is verantwoordelijk voor de continuïteit van de eigen bedrijfsprocessen.

**Medewerkers** zijn verantwoordelijk voor het zorgvuldig omgaan met persoonsgegevens en andere (vertrouwelijke) informatie/data waar zij uit hoofde van hun functie toegang toe hebben.

2) ENSIA staat voor: Eenduidige Normatiek Single Information Audit. Zie: https://www.vngrealisatie.nl/ensia
3) Het dreigingsbeeld gemeenten wordt jaarlijks uitgebracht door de informatiebeveiligingsdienst (IBD), zie www.informatiebeveiligingsdienst.nl

## Verantwoording

De gemeente verantwoordt zich over het taakveld informatieveiligheid door middel van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA-methodiek).

De verantwoording over informatieveiligheid komt tot uitdrukking in de jaarlijkse collegeverklaring Informatiebeveiliging en het gemeentelijk jaarverslag. Door middel van deze verantwoording wordt het bestuur geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente Maastricht informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar burgers adequaat te beschermen.

De gemeentesecretaris wijst een ENSIA-coördinator aan die in zijn opdracht ervoor zorgt dat de informatie die nodig is voor het beantwoorden van de ENSIA-vragenlijsten, wordt opgehaald bij de verantwoordelijke afdelingsmanagers.

## Evaluatie en herziening strategisch informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid wordt minimaal één keer per jaar en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bij- en opnieuw formeel vastgesteld.

*Aldus besloten door het college van burgemeester en wethouders van Maastricht d.d. 16 december 2025.*

*De Secretaris Wnd*
*K. Leonard*

*De Burgemeester,*
*W.A.G. Hillenaar*