



## Samenvatting

Met dit nieuwe strategisch informatiebeveiligingsbeleid gaat de gemeente Maastricht verder op de ingeslagen weg van verbetering van de beveiliging van (vertrouwelijke) informatie en persoonsgegevens binnen de gemeente. Het strategisch informatiebeveiligingsbeleid is richtinggevend en kader stellend en onverkort van toepassing op de hele gemeentelijke organisatie. Het strategisch informatiebeveiligingsbeleid sluit aan bij het nieuwe landelijke normenkader de baseline informatiebeveiliging overheid en de daarop gebaseerde 10 bestuurlijke principes voor informatiebeveiliging.

## Beslispunten

Vaststellen van het bijgaande strategisch informatiebeveiligingsbeleid onder gelijktijdige intrekking van het bestaande beleid uit 2015.

## Besluit Burgemeester en Wethouders d.d. 08-10-2019:

Conform.



## **1. Aanleiding**

Op grond van de Baseline Informatiebeveiliging Gemeenten (BIG) wordt het informatiebeveiligingsbeleid minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Het huidige beleid is inmiddels vier jaar oud, Bovendien wordt met ingang van 2020, de dit jaar nog geldende BIG, vervangen door de Baseline Informatie Beveiliging Overheid (BIO).

## **2. Context**

De Baseline Informatiebeveiliging Overheid (BIO) wordt met ingang van 2020 het nieuwe normenkader voor alle overheden. Deze vervangt de Baseline Informatiebeveiliging Gemeenten (BIG). De belangrijkste verschillen tussen de BIO en BIG zijn:

- Binnen de BIO wordt op basis van generieke schade en bedreigingen een onderscheid gemaakt in drie basisbeveiligingsniveaus (BBN) met bijbehorende beveiligingseisen.
- De BIO kent meer risicomanagement – Het lijnmanagement (de proceseigenaar) bepaalt per informatiesysteem het BBN.
- De BIO kent fors minder maatregelen – De ISO 27002:2013 norm bestaat uit 114 controls, ofwel beheersmaatregelen.
- Een deel van de controls is uitgewerkt in verplichte maatregelen (136) omdat deze voortvloeien uit wet- en regelgeving. De BIO noemt deze verplichte maatregelen ‘overheidsmaatregelen’.

## **3. Gewenste situatie**

Door middel van het vaststellen van het bijgevoegde informatiebeveiligingsbeleid inclusief bijlagen, komt het beleid van de gemeente Maastricht in lijn met de nieuwe landelijke norm, zijnde de Baseline Informatiebeveiliging Overheid (BIO).

## **4. Effect op duurzaamheid en/of gezondheid**

N.v.t.

## **5. Effect op de openbare ruimte**

N.v.t.

## **6. Personeel en organisatie**

N.v.t.



## **7. Informatiemanagement en automatisering**

Met de vaststelling van het nieuwe informatiebeveiligingsbeleid zijn de hierin opgenomen controls en maatregelen, uitgangspunten die zowel voor de bestaande inrichting als voor nieuwe initiatieven op het gebied van informatie en automatisering gelden.

## **8. Financiën**

Het vaststellen van dit Strategisch Informatiebeveiligingsbeleid past binnen de bestaande begroting en kost geen extra geld. Aan de implementatie van eventuele maatregelen uit dit beleid kunnen wel kosten vastzitten. Implementatie van deze (structurele) maatregelen in de toekomst behoren tot de reguliere bedrijfsvoering en daarbij behorende budgetten. Dit zijn keuzes en budgetaanvragen/reserveringen die t.z.t. casuïstiek gemaakt zullen moeten worden door het verantwoordelijke (lijn)management. Projectmatige initiatieven worden opgenomen in het (meer)jaarlijkse I&A-plan. In dat geval vindt dekking plaats via het project, hetgeen ook geen extra budgetaanvraag voor de begroting met zich meebrengt.

## **9. Aanbestedingen**

N.v.t.

## **10. Participatie tot heden**

N.v.t.

## **11. Voorstel**

Vaststellen van het bijgaande strategisch informatiebeveiligingsbeleid onder gelijktijdige intrekking van het bestaande beleid uit 2015.

## **12. Uitvoering, evaluatie en vervolg**

De uitvoering van het strategisch informatiebeveiligingsbeleid krijgt gestalte in het op te stellen (meer)jaarlijks informatiebeveiligingsplan en in de gemeentebrede bewustwordingscampagne voor het personeel.